

ATTORNEY DOCKET NO.  
062891.0292

12-02-05  
PATENT APPLICATION  
09/477,193

1



**In the United States Patent and Trademark Office  
on Appeal from the Examiner to the Board  
of Patent Appeals and Interferences**

In re Application of: James R. Tighe, et al.  
Serial No.: 09/477,193  
Filing Date: January 4, 2000  
Group Art Unit: 2136  
Examiner: Carl G. Colin  
Title: SYSTEM AND METHOD FOR PROVIDING SECURITY IN  
A TELECOMMUNICATION NETWORK

**MAIL STOP APPEAL BRIEF - PATENT**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Dear Sir:

**Appeal Brief**

Appellants have appealed to the Board of Patent Appeals and Interferences ("Board") from the decision of the Examiner mailed September 27, 2005, finally rejecting all pending Claims 1-6, 8-30, and 32-45. Appellants filed a Notice of Appeal on November 22, 2005, with the statutory fee of \$500.00.

12/05/2005 MBIZUNES 00000051 09477193

01 FC:1402

500.00 OP

**Real Party In Interest**

This Application is currently owned by Cisco Technology, Inc. as indicated by:

an Assignment recorded on January 4, 2000, from the inventor to Cisco Technology, Inc., in the Assignment Records of the PTO at Reel 010519, Frame 0462 (7 pages).

**Related Appeals and Interferences**

To the knowledge of Appellants' counsel, there are no known interferences or judicial proceedings that will directly affect or be directly affected by or have a bearing on the Board's decision regarding this Appeal.

**Status of Claims**

Claims 1-6, 8-30, and 32-45 are pending in this Application, stand rejected pursuant to a final Office Action mailed September 27, 2005 (the "Final Office Action"), and are all presented for appeal. Claims 7 and 31 were cancelled in a Response to Office Action mailed on May 17, 2004. All pending claims are shown in Appendix A, attached hereto, along with an indication of the status of those claims.

**Status of Amendments**

All amendments submitted by Appellants have been entered by the Examiner.

**Summary of Claimed Subject Matter**

FIGURE 1 illustrates an exemplary communication network 10. In the illustrated embodiment, communication network 10 includes a plurality of local area networks (LANs) 20, 30, 40 that are interconnected using various techniques, including the Internet 50 and a wide area network (WAN) 60. Each LAN is a computer data network that is further operable to transmit audio and/or video telecommunication signals. Communication network 10 also includes a remote communication site 70 coupled to one or more of LANs 20, 30, 40 using the Public Switched Telephone Network (PSTN) 80. (Page 6, lines 2-12).

IP telephony devices, such as an IP telephone, can be coupled to any of these IP networks and used for communication between users of the networks. Furthermore, since all IP networks share a common method of transmitting data, telecommunication signals may be transmitted between telephony devices that are located on different, but interconnected, IP networks. The technology that allows telecommunications to be transmitted over an IP network may be referred to as Voice over IP (VoIP). As an example, IP telephony devices 24 are coupled to LAN 20 to allow communication over LAN 20. IP telephony devices 24 have the capability of encapsulating a user's voice (or other inputs, such as the user's image) into IP packets so that the voice can be transmitted over LANs 20, 30, 40, Internet 50, WAN 60, and/or PSTN 80. IP telephony devices may include telephones, fax machines, computers running telephony software (such as MICROSOFT NETMEETING), gateways, or any other device capable of performing telephony functions over an IP network. For the purposes of this application, all types of telephony devices (both IP and non-IP) will be referred to as "telephones." (Page 7, line 25 through Page 8, line 14).

A call manager 26 controls IP telephones 24 on LAN 20. Call manager 26 is an application that controls call processing, routing, telephone features and options (such as call hold, call transfer and caller ID), device configuration, and other telephony functions and parameters within communication network 10. Call manager 26 can control all of the IP telephones 24 on LAN 20, and it may also control IP telephones on other IP networks. For example, call manager 26 is capable of controlling IP telephones 32 on LAN 30 and IP telephones 42 on LAN 40. (Page 8, line 31 through Page 9, line 9).

When a user wishes to place a call from an IP telephone 24a on LAN 20 to another IP telephone 24b on LAN 20 (an intra-LAN call), the calling telephone transmits a signal to call

manager 26 indicating the desired function and the telephone to be called. Call manager 26 then checks on the availability of the called telephone and, if available, establishes the call by instructing the calling (originating) telephone to begin audio and/or video (media) streaming to the called (destination) telephone. The initial signaling between call manager 26 and either the originating telephone or the destination telephone is transmitted over LAN 20 using the Transmission Control Protocol (TCP). The TCP network layer in the transmitting telephone divides the data to be transmitted into one or more packets, numbers the packets, and then forwards them to the IP network layer for transmission to the destination telephone. Although each packet has the same destination IP address, the packets may travel along different paths to reach the intended destination. As the packets reach the destination telephone, the TCP layer of the destination telephone reassembles the individual packets and ensures that they all have arrived. Once TCP reassembles the data, it forwards the data to the destination telephone as a single message. (Page 9, line 10 through Page 10, line 2).

After call manager 26 initiates the call with signaling via TCP, audio streaming between the telephones begins. A codec (coder/decoder) converts the voice, video or fax signals generated by the users of the telephones from analog voice signals into digital form. The codec may be implemented either in software or as special-purpose hardware in IP telephones 24. In the case of an IP telephone, as the user speaks into the handset, the codec converts the analog voice signals into digital data. The digitally encoded data is then encapsulated into IP packets so that it can be transmitted over LAN 20. (Page 10, lines 3-13).

. . . [W]hen a call is placed to an IP telephone, for example IP telephone 24, a call initiation request is first sent to call manager 26. If the originating telephone is an IP telephone (e.g., a telephone on LAN 30, LAN 40, Internet 50, or WAN 60), the originating IP telephone generates the call initiation request and sends the request to call manager 26. If the originating telephone is a non-IP telephone, such as telephone 74, gateway 22 first intercepts the incoming call from PSTN 80, and then sends a call initiation request to call manager 26 indicating the IP telephone that is being called. In either case, once call manager 26 receives the call initiation request, call manager 26 sends a signal to the destination IP telephone offering the call to the telephone. (Page 12, line 31 through Page 13, line 14).

One advantage associated with IP telephones is their ability to communicate and interact with any other IP device coupled to the IP network. For example, IP telephones may interact and communicate with other IP telephones, with non-telephony IP devices, and even

with virtual telephony devices. A virtual telephony device may be implemented as software, firmware and/or hardware to interact with devices in communication network 10. Virtual telephony devices may be implemented as software or firmware on any existing or dedicated device on the IP network. For example, computer 27 contains software for implementing one or more virtual telephony devices 28. Virtual telephony device software may also be located at call manager 26, or any other network device. The computer or other device on which the virtual telephony software is located includes a network interface, a memory to store the software, and a processor to execute the software. (Page 14, lines 5-21).

Virtual telephony devices 28 may be logically inserted between two or more telephones to act as an intermediary between the two telephones. Once such a relationship is established, signaling and media streaming that passes through virtual telephony device 28 may then be modified through address translation or media stream manipulation for various reasons before they are sent on to the destination device. Reasons for such modifications include duplicating streams, dynamically redirecting streams, maintaining connections between devices, converting between data formats (e.g., A-Law to  $\mu$ -Law), and injecting media. (Page 14, line 22 through Page 15, line 2).

As will be described in the present application, one implementation of virtual telephony device 28 is as a telephony proxy to allow telecommunications between a trusted telephone coupled to a protected network, such as LAN 20, and an untrusted device external to the protected network while still maintaining network security. Through the use of an authentication controller 25, which evaluates incoming communications, the telephony proxy can be used to monitor communications directed to trusted telephones on LAN 20, for example, from untrusted devices outside of LAN 20 (e.g., telephones coupled to LAN 40 or Internet 50). The telephony proxy may also be used to manipulate the media streaming between the trusted telephone and the untrusted device as required to maintain the integrity of the protected network. (Page 15, lines 3-17).

In order for a call to be placed through a virtual telephony device, for example a call placed to IP telephone 24a in LAN 20 through virtual telephony device 28, telephone 24a should be registered with virtual telephony device 28. Telephone 24a is instructed by call manager 26 to register with virtual telephony device 28 at a specified IP address and port. Telephone 24a signals virtual telephony device 28 via TCP/IP indicating that it would like to register. If virtual telephony device 28 accepts the registration request, telephone 24a sends a



registration message to virtual telephony device 28 using TCP/IP. The registration message typically comprises information about the telephone such as the telephone's IP and media access control (MAC) addresses, the type of telephone, and the codec(s) used by the telephone. (Page 15, lines 3-17).

FIGURE 2 illustrates an exemplary communication link created using virtual telephony device 28. The communication link represents any connection or other coupling between two or more telephony devices that allows the telephony devices to communicate in some manner. It should also be noted that although the TCP and UDP protocols are specifically identified in the following discussion, any other suitable signaling and media transmission protocols may be used. Virtual telephony device 28 initiates this communication link by first creating a logical connection to telephone 24a. Creating this logical connection involves associating logical UDP and TCP ports of virtual telephony device 28 with telephone 24a. Virtual telephony device 28 designates a TCP port (for example, port 2000) as the signaling port of telephone 24a and designates a UDP port (for example, port 2100) as the streaming port of telephone 24a. Virtual telephony device 28 instructs call manager 26 to send all signaling directed to telephone 24a to logical port 2000 of virtual telephony device 28. Likewise, virtual telephony device 28 instructs call manager 26 to send all media streaming directed to telephone 24a from other telephones to logical port 2100 of virtual telephony device 28. Virtual telephony device 28 will automatically forward any data that is subsequently sent to these ports of virtual telephony device 28 to the IP address of telephone 24a (for example 200.50.10.1). As far as call manager 26 is concerned, telephone 24a is located at these logical ports of virtual telephony device 28. (Page 16, lines 3-31).

Likewise, virtual telephony device 28 has typically designated a TCP port (for example, port 1000) as the signaling port of call manager 26 (data is typically not streamed to and from call manager 26, so a UDP port is usually not required). Virtual telephony device 28 instructs telephone 24a (as well as any other registered telephones) to send all signaling directed to call manager 26 to logical port 1000 of virtual telephony device 28. (Page 17, lines 1-8).

Since all data that is sent between two IP telephones may be passed through virtual telephony device 28, virtual telephony device 28 can be used for other purposes in addition to the address translation function described above. For example, virtual telephony device 28 may serve as a telephony proxy to facilitate telecommunications between a "trusted device"

located in the same network as the telephony proxy and an "untrusted device" located outside the network. In this case, communications between the trusted device and the untrusted device are routed through the telephony proxy after being authenticated. (Page 19, lines 7-17).

For the purposes of this application the term "trusted device" will be used to indicate an IP telephone that is coupled to a protected or trusted IP network(s) being serviced by the telephony proxy, such as telephone 24b on LAN 20. The term "untrusted device" will be used to indicate an IP or non-IP device that is external to the protected IP network(s). The untrusted device may be coupled to an untrusted network, such as telephone 52 on Internet 50. Alternatively, the untrusted device may be a telephone coupled to a trusted network, such as telephone 32 on LAN 30. In this case, the telephone is untrusted to telephony proxy 28, for example, because the trusted network (LAN 30) is coupled to the protected network (LAN 20) using an untrusted network, such as Internet 50. (Page 19, lines 18-31).

Telephony proxy 28 operates like virtual telephony device 28, described in FIGURE 2, to facilitate a telephone call between two or more telephones. However, because at least one of the telephones is untrusted when telephony proxy 28 is used, an authentication step is required before a telecommunication link can be established between the telephones. This authentication step is performed by authentication controller 25. Thus, the primary difference between the telephony proxy software and the virtual telephony device software is that the telephony proxy software does not establish a telecommunication link between a trusted device and an untrusted device until authentication controller 25 approves the link. (Page 20, lines 9-21).

When a call initiation request is made by an untrusted device to a trusted device (the term "trusted device" being used to indicate the target of a call initiation request before the request is authenticated), authentication controller 25 evaluates this request to determine if a telecommunication link should be established between the trusted device and the untrusted device using telephony proxy 28. Various methods of evaluating the call initiation request, such as an address look-up or a message format analysis, are described below in conjunction with FIGURE 3. As with telephony proxy 28, authentication controller 25 may be implemented as software on any device in LAN 20. For example, the authentication software may be located on a dedicated computer, or it may be located on a computer having other purposes such as computer 26 running the call manager software or computer 27 running the

telephony proxy software. In one embodiment, the call manager software, the authentication software, and the telephony proxy software may all be running on the same computer. (Page 20, line 22 through Page 21, line 9).

FIGURE 3 illustrates an exemplary method for using a virtual telephony proxy to facilitate a telephone call between a trusted device and an untrusted device. The method begins when a call initiation request is received from an untrusted device at step 102, indicating a desire to place a telephone call to a trusted device . . . The call initiation request may comprise any indication that the untrusted device would like to communicate with a trusted device . . . Once the call initiation request has been received, the request is transferred to authentication controller 25 at step 104 . . . The call initiation request is evaluated by authentication controller 25 at step 106. A variety of evaluations may be performed on the call initiation request to determine whether the request should be accepted and whether a call should be established between the untrusted device and the trusted device. (Page 21, line 10 through Page 22, line 17).

One such evaluation involves determining whether the trusted device is a proper recipient of a telephone call from an untrusted device. This evaluation may simply involve determining whether the trusted device is actually a telephone or some other telephony device capable of receiving telephone calls. Since IP telephony allows the integration of telephones and other network devices on the same IP network, care must be taken to ensure that unauthorized parties are not able to access secured data or send unwanted data, such as a virus, to the network. (Page 22, lines 18-27).

One way that authentication controller 25 can determine whether the trusted device is actually a telephone is by comparing the network address of the called device with the addresses on an address list 23 stored in the memory of the computer running the authentication controller software (or in the memory of any other network device). For example, the approved address list may contain the IP addresses of telephones and other telephony devices that are permitted to receive calls from untrusted devices. Alternatively, address list 23 list may contain the IP addresses of untrusted devices that are either authorized to communicate with trusted devices or that are prohibited from communicating with trusted devices. Address list 23 may contain either individual or subnet addresses. (Page 23, lines 11-24).

Once authentication controller 25 has evaluated the call initiation request, it determines the appropriate action to take at step 108 based on whether the evaluation was positive or negative. If the evaluation is negative, for example, if the trusted device to which the call is directed is not actually a telephone or other proper recipient of an incoming call, then authentication controller 25 denies the call initiation request at step 110. Once the request is denied, call manager 26 will not attempt to establish a telecommunication link between the untrusted device and the trusted device. (Page 23, line 25 through Page 24, line 4).

If the evaluation of the call initiation request is positive, then authentication controller 25 transmits a signal to call manager 26 authorizing a telephone call between the trusted device and the untrusted device at step 112. In response to this signal, call manager 26 establishes a telecommunication link between the trusted device and the untrusted device at step 114. This telecommunication link, as described above in conjunction with FIGURE 2, may be established such that all telecommunications between the trusted device and the untrusted device are communicated through telephony proxy 28. (Page 24, line 5 through Page 24, line 16).

Assuming that the trusted device is registered with telephony proxy 28 (as described above), call manager 26 instructs the untrusted device to begin media streaming to the logical port of telephony proxy 28 that has been associated with the trusted device. Additionally, call manager 26 instructs telephony proxy 28 to associate another of its logical ports with the untrusted device. In the manner described above, telephony proxy 28 changes the information in header of the packets incoming from the untrusted device by altering the source address and source port to the address of telephony proxy 28 and the logical port of telephony proxy 28 that was associated with the untrusted device (note that the address may be in the IP header and the port may be in the UDP or TCP header). Telephony proxy 28 then forwards the packets to the trusted device, so that the packets appear to be sent from telephony proxy 28. A similar address translation process is performed on packets being sent from the trusted device to the untrusted device, as described above. (Page 24, line 17 through Page 25, line 4).

The continuous address translation by telephony proxy 28 ensures that all communications between the trusted device and the untrusted device are controlled by telephony proxy 28. Such continuous control prevents the untrusted device from determining the actual network address of the trusted device. (Page 25, lines 5-10).

In one embodiment, telephony proxy 28 also continuously monitors the media streaming between the trusted device and the untrusted device at step 315. For example, telephony proxy 28 can ensure that the media streaming is in a recognized audio encoding format, such as G.711, G.723, or G.729. Telephony proxy 28 can also ensure that the communications between the trusted device and the untrusted device are, in fact, media streaming (or more specifically, RTP media streaming). Furthermore, any other appropriate methods of evaluating the media streaming, including appropriate techniques implemented by data firewalls, may also be used to monitor any unauthorized access to a network. If telephony proxy 28 determines at any point that suspect media streaming or other transmissions are occurring, telephony proxy 28 can manipulate or terminate the data streaming between the untrusted device and the trusted device. Once the telephone call between the trusted device and the untrusted devices is completed (or once suspect transmissions are detected), the telecommunication link is terminated at step 116. (Page 25, lines 11-30).

With regard to the independent claims currently under Appeal, Appellants provide the following concise explanation of the subject matter recited in the claim elements. For brevity, Appellants do not necessarily identify every portion of the Specification and drawings relevant to the recited claim elements. Additionally, this explanation should not be used to limit Appellants' claims but is intended to assist the Board in considering the Appeal of this Application.

For example, independent Claim 1 recites the following:

A method for establishing a telephone call between a trusted Internet Protocol (IP) telephone and an untrusted device (e.g., Page 15, lines 3-17; Page 19, line 7 through Page 21, line 9), the method comprising:

receiving a call initiation request from an untrusted device external to a trusted network, the call initiation request indicating a desired communication with a trusted IP telephone coupled to the trusted network (e.g., Page 12, line 31 through Page 13, line 13; Page 20, line 22 through Page 21, line 9; Page 21, line 21 through Page 22, line 4);

evaluating the call initiation request (e.g., Page 20, line 22 through Page 21, line 9; Page 22, line 5 through Page 24, line 4);

establishing a telecommunication link between the untrusted device and the trusted IP telephone in response to a positive evaluation of the call initiation request, wherein evaluating the call initiation request comprises determining whether the untrusted device is requesting the establishment of media streaming with the trusted IP telephone (e.g., Page 13, line 14 through Page 14, line 4; Page 22, line 5 through Page 24, line 16);

monitoring communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network (e.g., Page 25, lines 11-30); and

terminating the telecommunication link if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming to maintain the integrity of the trusted network (e.g., Page 25, lines 11-30);

wherein establishing the telecommunication link comprises:

associating a first logical port of a telephony proxy with the trusted IP telephone (e.g., Page 16, lines 11-31; Page 17, lines 14-29; Page 24, lines 17-21);

associating a second logical port of the telephony proxy with the untrusted device (e.g., Page 24, lines 21-23);

receiving first telecommunication data from the untrusted device at the first logical port (e.g., Page 24, lines 17-21);

modifying a first source address information in the first telecommunication data to specify the second logical port of the telephony proxy (e.g., Page 24, lines 23-30);

communicating the first telecommunication data with the modified first source address information to the trusted IP telephone (e.g., Page 24, line 30 through Page 25, line 2);

receiving second telecommunication data from the trusted IP telephone at the second logical port (e.g., Page 25, lines 2-10);

modifying a second source address information in the second telecommunication data to specify the first logical port of the telephony proxy (e.g., Page 17, line 30 through Page 18, line 18; Page 25, lines 2-10); and

communicating the second telecommunication data with the modified second source address information to the untrusted device (e.g., Page 25, lines 2-10).

**Grounds of Rejection to be Reviewed on Appeal**

Are Claims 1-6, 8-30, 32-42, and 43-45 patentable over the Examiner's proposed combinations of U.S. Patent No. 5,455,855 to Hokari et al. ("*Hokari*") in view of European Patent Publication EP 841831 A2 to Civanlar et al. ("*Civanlar*") and U.S. Patent No. 6,389,462 issued to Cohen et al. ("*Cohen*") under 35 U.S.C. § 103(a)?

**Grouping of Claims**

Appellants have made an effort to group claims to reduce the burden on the Board. In the Argument section of this Appeal Brief, where appropriate, Appellants present arguments as to why particular claims subject to a ground of rejection are separately patentable from other claims subject to the same ground of rejection. To reduce the number of groups and thereby reduce the burden on the Board, Appellants do not argue individually every claim that recites patentable distinctions over the references cited by the Examiner, particularly in light of the clear allowability of Appellants' independent claims.

The claims of each group provided below may be deemed to stand or fall together for purposes of this Appeal. The claims may be grouped together as follows for purposes of this Appeal:

1. Group 1 may include independent Claims 1, 2, 14, 26, and 38 and dependent Claims 3, 6, 8-11, 13, 15-20, 23-25, 27, 30, 31-35, 37, 40-43, and 45;
2. Group 2 may include dependent Claims 4, 28, and 39;
3. Group 3 may include dependent Claims 5 and 29;
4. Group 4 may include dependent Claims 12, 36, and 44; and
5. Group 5 may include dependent Claims 21.



**Argument:**

**The Claims are Patentable over the Proposed *Hokari-Civanlar-Cohen*  
and *Hokari-Civanlar* Combinations**

Claims 1-6, 8-30, and 32-45 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over various combinations of *Hokari*, *Civanlar*, and *Cohen*. A copy of *Hokari* is attached as Appendix B, and a copy of *Civanlar* is attached as Appendix C. A copy of *Cohen* is attached as Appendix D. Appellants respectfully submit that the Examiner's proposed combinations of *Hokari*, *Civanlar*, and *Cohen* fail to support the obviousness rejections of these claims. Appellants respectfully submit that these rejections are therefore improper and should be reversed by the Board.

**I. Standard**

The question raised under 35 U.S.C. § 103 is whether the prior art taken as a whole would suggest the claimed invention taken as a whole to one of ordinary skill in the art at the time of the invention. *See* 35 U.S.C. § 103(a). Accordingly, even if all elements of a claim are disclosed in various prior art references, which is certainly not the case here as discussed below, the claimed invention taken as a whole cannot be said to be obvious without some reason given in the prior art why one of ordinary skill in the art at the time of the invention would have been prompted to modify the teachings of a reference or combine the teachings of multiple references to arrive at the claimed invention.

The M.P.E.P. sets forth the strict legal standard for establishing a *prima facie* case of obviousness based on modification or combination of prior art references. "To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references where combined) must teach or suggest all the claim limitations." M.P.E.P. § 2142, 2143. The teaching, suggestion or motivation for the modification or combination and the reasonable expectation of success must both be found in the prior art and

cannot be based on an Appellants' disclosure. *See Id.* (citations omitted). "Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art" at the time of the invention. M.P.E.P. § 2143.01. Even the fact that references *can* be modified or combined does not render the resultant modification or combination obvious unless the prior art teaches or suggests the desirability of the modification or combination. *See Id.* (citations omitted). Moreover, "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. All words in a claim must be considered in judging the patentability of that claim against the prior art." M.P.E.P. § 2143.03 (citations omitted).

The governing Federal Circuit case law makes this strict legal standard even more clear.<sup>1</sup> According to the Federal Circuit, "a showing of a suggestion, teaching, or motivation to combine or modify prior art references is an essential component of an obviousness holding." *In re Sang-Su Lee*, 277 F.3d 1338, 1343, 61 U.S.P.Q.2d 1430, 1433 (Fed. Cir. 2002) (quoting *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25, 56 U.S.P.Q.2d 1456, 1459 (Fed. Cir. 2000)). "Evidence of a suggestion, teaching, or motivation . . . may flow from the prior art references themselves, the knowledge of one of ordinary skill in the art, or, in some cases, the nature of the problem to be solved." *In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). However, the "range of sources available . . . does not diminish the requirement for actual evidence." *Id.* Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." *In re Mills*, 916 F.2d at 682, 16 U.S.P.Q.2d at 1432. *See also In re Rouffet*, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1457-58 (Fed. Cir. 1998) (holding a *prima facie* case of obviousness not made where the combination of the references taught every element of the claimed invention but did not provide a motivation to combine); *In Re Jones*, 958 F.2d 347, 351, 21 U.S.P.Q.2d 1941, 1944 (Fed. Cir. 1992) ("Conspicuously missing from this record is any evidence, other than the PTO's speculation (if that can be called evidence) that one of ordinary skill in the herbicidal art would have been motivated to make the modification of the prior art salts

<sup>1</sup> Note M.P.E.P. 2145 X.C. ("The Federal Circuit has produced a number of decisions overturning obviousness rejections due to a lack of suggestion in the prior art of the desirability of combining references.").

necessary to arrive at” the claimed invention.). Even a determination that it would have been obvious to one of ordinary skill in the art at the time of the invention to try the proposed modification or combination is not sufficient to establish a *prima facie* case of obviousness. *See In re Fine*, 837 F.2d 1071, 1075, 5 U.S.P.Q.2d 1596, 1599 (Fed. Cir. 1988).

In addition, the M.P.E.P. and the Federal Circuit repeatedly warn against using an Appellants’ disclosure as a blueprint to reconstruct the claimed invention. For example, the M.P.E.P. states, “The tendency to resort to ‘hindsight’ based upon applicant’s disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.” M.P.E.P. § 2142. The governing Federal Circuit cases are equally clear. “A critical step in analyzing the patentability of claims pursuant to [35 U.S.C. § 103] is casting the mind back to the time of invention, to consider the thinking of one of ordinary skill in the art, guided only by the prior art references and the then-accepted wisdom in the field. . . . Close adherence to this methodology is especially important in cases where the very ease with which the invention can be understood may prompt one ‘to fall victim to the insidious effect of a hindsight syndrome wherein that which only the invention taught is used against its teacher.’” *In re Kotzab*, 217 F.3d 1365, 1369, 55 U.S.P.Q.2d 1313, 1316 (Fed. Cir. 2000) (citations omitted). In *In re Kotzab*, the Federal Circuit noted that to prevent the use of hindsight based on the invention to defeat patentability of the invention, the court requires the Examiner to show a motivation to combine the references that create the case of obviousness. *See id.* *See also, e.g., Grain Processing Corp. v. American Maize-Products*, 840 F.2d 902, 907, 5 U.S.P.Q.2d 1788, 1792 (Fed. Cir. 1988). Similarly, in *In re Dembiczak*, the Federal Circuit reversed a finding of obviousness by the Board, explaining that the required evidence of such a teaching, suggestion, or motivation is essential to avoid impermissible hindsight reconstruction of an applicant’s invention:

Our case law makes clear that the best defense against the subtle but powerful attraction of hind-sight obviousness analysis is *rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references*. Combining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor’s disclosure as a

blueprint for piecing together the prior art to defeat patentability—the essence of hindsight.

175 F.3d at 999, 50 U.S.P.Q.2d at 1617 (emphasis added) (citations omitted).

## **II. The *Hokari* Reference**

The *Hokari* reference which discloses a system for connecting a public network subscriber and a private network subscriber in ISDN to make communications possible between them, is comprised of a first exchange for connecting the public network subscriber and the public network, a second exchange for the private network subscriber and the private network, and a plurality of third exchanges for connecting a public line of the public network and a private line of the private network. (Column 2, lines 14-21).

The private branch exchanges (PBXs) 102-104 are connected with the public network of the Integrated Services Digital Network (ISDN) 101. Of them, the PBXs 103 and 104 are also connected with a leased line network or virtual private network 105. The leased line network 105 may be a privately owned network or a software defined network (SDN). The PBXs 102 and 103 are located in Tokyo and the PBX 104 is located in Osaka. The ISDN numbers "03-3210-2222" and "03-3210-1111" are assigned to the PBXs 102 and 103, respectively. Furthermore, in the leased line network 105, the leased line numbers "8-11-5000" and "8-10-2000" are assigned to the PBXs 103 and 104, respectively. (Column 3, lines 31-43).

When a dial number is received from the public network subscriber 106 (S1021), the PBX 102 decides whether the dial number is a leased line number or not (S1022). If the dial number received is a leased line number (YES of S1022), a set-up message 301 for the public line--leased line connection is formed (S1023-S1025). If it is an ISDN public network number (NO of S1022), a set-up message of the ISDN public network is formed (S1027). Such a setup message formed in this way is transmitted from the PBX 102 to the ISDN public network 101 (S1026). (Column 4, lines 12-23).

Suppose that, when the top number of the dial number is "8", the dial number is a leased line number, and when it is other than "8", the dial number is an ISDN public network number. And further suppose that the public network subscriber 106 dials the number "8-10-2000" of the leased line network subscriber 107 where the dial number "8" is a special service

code, the dial number "10" is a leased line number, and the dial number "2000" is an extension number. (Column 4, lines 24-31).

Therefore, on receipt of the dial number "8-10-2000", the PBX 102 decides that it is a leased line number (YES of S1022), and forms the set-up message for the public line--leased line connection, as mentioned bellow (S1023-S1025). (Column 4, lines 32-36).

The control unit 226 of the PBX 102 selects the nearest PBX 103 as an access point to the leased line network 105 by referring to the selection signal conversion table of the main memory 227, and sets the destination number of the set-up message 301 at the ISDN number "03-3210-1111" of the PBX 103 (S1023). Furthermore, the control unit 226 sets the destination sub-address at the dialed number "8-10-2000" of the called party (S1024), and the number of the calling party at the ISDN number "03-3210-2222" of the calling party 106 (S1025). Such a set-up message 301 for the public line--leased line connection is sent to the ISDN public network 101 (S1026). FIG. 4 shows the set-up message 301. (Column 4, lines 37-50).

Then, as shown in FIG. 6, the PBX 103 which becomes an access point receives the set-up message 301 having the destination number which is identical to the stored public line--leased line connection number "03-3210-1111" from the ISDN public network 101 (S1030). The access point PBX 103 decides whether the calling party number "03-3210-2222" of the calling subscriber 106 is registered in the ID table of the main memory 327 (S1031). If it is registered (YES of S1031), the connection of the call is permitted (S1032) and the leased line number "8-10-2000" is read out from the destination sub-address of the set-up message (S1033). Then, a new set-up message having this leased line number as a destination number is formed and sent to the leased line network 105 to connect the call. The transit connection is made between the calling party 106 and the called party 107 through the ISDN public network 101 and the leased line network 105 (S1034). (Column 4, lines 51-67).

On the other hand, if the calling party 106 is not registered in the ID table of the PBX 103 (NO of S1031), the connection of the call is not permitted and the call is disconnected (S1035). Therefore, only specific calling subscribers can access to the leased line network 105 without dialing a special ID code, and the security of the leased line network 105 can be maintained. (Column 5, lines 1-7).

### III. The *Civanlar* Reference

The *Civanlar* reference discloses an apparatus for establishing communications paths over a circuit switched network, a connectionless packet switched network, and a connection-oriented packet switched network, and more particularly to an apparatus for establishing point-to-point or point-to-multipoint audio or video communication over a telephony network, the Internet, and an Asynchronous Transfer Mode (ATM) or a Frame Relay (FR) network. (Column 1, lines 5-13).

In accordance with the principles of the invention . . . a WAN-based Voice Gateway [is provided] which connects to the telephony network, the Internet and the ATM/FR network. Given that network users will be in communication with a variety of such heterogeneous networks, gateway capabilities will be needed between them to support end-point stations in a voice session which are connected to one or more of these different networks. The telephony network, Internet and FR/ATM Networks all use different schemes for establishing a voice session (i.e., call set-up protocols), and different formats for controlling a session and transporting voice. The gateway of the present invention provides conversion of the transmission format, control, call signaling and audio stream (and potentially video and data streams) between different transmission standards. The capabilities of the gateway may also include audio coding translation (e.g., between G.722 and G.728) and address translation between different address types (e.g., a telephone number and an IP address). (Column 3, lines 29-49).

As seen in FIG. 4, an IP call set-up interface 101 is provided for receiving and terminating call-setup requests from the Internet and for generating call-set up requests to the Internet to establish connections between two or more Internet stations, telephony stations, frame relay stations, and/or ATM stations. Interface 101 sends and receives call setup requests in the form of IP packets using signaling protocols such as Q.931 (or a sub-set of Q.931 as defined in H.323) or another signaling protocol that may be developed particularly for transmitting voice over IP. The IP call set-up interface 101 receives call-setup requests from the telephony call set-up interface 102 (discussed below) in the form of DTMF, Q.931 or other signaling standards. The interface 101 also receives call-setup requests from the ATM/FR call set-up interface 103 if the call-setup request is in the form of Q.2931. A signaling format translator 104 is provided to translate the call-setup requests into a form that

the interface 101 can properly understand. The translation is performed before the requests are forwarded to the IP call set-up interface 101. The interface 101 monitors the status of each call establishment session and transmits error messages, as appropriate, in the form of audio messages or digital data to each IP station participating in the session. (Column 5, line 50 through Column 6, line 17).

The gateway 100 also includes a telephony call set-up interface 102 for receiving call-setup requests from the telephony network 52 or sending call-setup requests to the telephony network 52 to establish connections between two or more Internet stations, telephony stations, frame relay stations and/or ATM stations. Telephony set-up interface 102 receives and sends call setup messages in accordance with Q.931 or with other telephony signaling protocols. The interface 102 also generates SS7 signaling messages to a Network Control Point (NCP) to obtain, for example, a telephone number translation prior to generating an outgoing Q.931 signaling message to the telephony network 52. Additionally, telephony call set-up interface 102 receives call-setup requests from the IP call set-up interface 101 and the ATM/FR call set-up interface 103 if the call setup request originates in one [of] these networks. The signaling format translator 104 translates the call-set up into a form that is understood by the telephony call set-up interface 102. (Column 6, lines 18-37).

FIG. 6 shows a flow chart of an exemplary method for establishing a voice session between the user stations 300 and 600 of FIG. 3 in accordance with the principles of this invention. As seen in FIG. 3, station 300 is provided with direct connectivity to the Internet via voice gateway B. Station 600 communicates with the voice gateway C via an N-ISDN interface. In FIG. 3, the voice gateways A, B and C are all "peers" and any local gateways attached thereto serve as "slaves." (Column 8, lines 50-58).

The method begins at step 501 when station 300 sends a call signaling request over the Internet to voice gateway B in the form of an IP packet. The IP packet carries signaling information (e.g., in the form of a Q.931 message), including the IP address of the called station 600. In step 503, the IP call set-up interface 101 parses the IP packet and retrieves the IP address of station 600. In step 505, the IP call set-up interface 101 sends an address query to the address translator 105 to retrieve other addresses for station 600. In step 511, the address translator 105 maps the IP address of station 600 to a toll-free 800 number. Thereafter, at the conditional branch point 513, address translator 105 determines if the 800 number of station 600 is served by voice gateway B. (Column 9, lines 1-15).

If the result in step 513 is no, indicating that voice gateway C serves station 600, the method continues with step 523 in which the address translator 105 returns to gateway B to retrieve the IP address of Voice Gateway C for contacting station 600. This step implies that the call to station 600 should be forwarded to voice gateway C, which is the “master” gateway responsible for serving station 600. Thereafter, in step 503, the IP call set-up 101 interface of Voice Gateway B routes the call to the IP call set-up interface 101 of Voice Gateway C for further processing. The method then continues as described below. (Column 9, lines 16-27).

If the result in step 513 is YES, indicating that voice gateway B serves the 800 number of station 600, the address translator interface 105 sends the 800 number to the IP call set-up interface 101 of gateway B in step 515. In step 517, the IP set-up interface 101 of gateway B sends the 800 number to the signaling format interface 105, which in turn constructs an SS7 message and forwards it to the telephony call set-up interface 102. In step 519, the interface 102 sends the SS7 message to the NCP in the signaling network to translate the 800 number into a telephone number. The NCP provides the requested telephone number to the telephony call set-up interface 102. Once the proper telephone number is determined, interface 102 sends a Q.931 message to station 600 in step 521 to establish the call. (Column 9, lines 28-42).

Once the station 600 is connected, across the Telephony Bridge 202 and IP Mixer 201, a control plane connection is first established between the Users 300 and 600 in step 601 (note that this connection traverses both Voice Gateway C and Voice Gateway B). This connection is employed by both stations in step 603 to indicate their respective audio encoding preferences, say G.711 for station 300 and G.723 for station 600. Additionally, note that the format translation between station 300 and station 600 on the connection plane occurs in voice gateway C (given that communication from voice gateway C to voice gateway B uses IP as the network layer protocol). Once the station capabilities and preferences are known to each voice gateway in step 605, the session managers 304 in both gateways B and C store a conference table that includes the preferences of both users. Communication proceeds between stations 300 and 600 in step 611 when station 300 sends a voice packet to the IP mixer 201 in gateway B, which in turn sends the packet to the IP mixer 201 in voice gateway C. (Column 9, line 43 through Column 10, line 11).



#### **IV. The *Cohen* Reference**

The *Cohen* reference relates to packet-switched computer networks, and more particularly, to a method and apparatus in such a network for transparently intercepting client web requests and redirecting them to proxy caches. (Column 1, lines 6-9). By modifying the GET request at the proxy redirector to include the destination address of the origin server, the number of bytes at the IP level in the packet containing the resultant absolute address are increased by the number of bytes in the prefix. Included in the header within each packet is a sequence number (seq) that provides an indication of the position of the first byte number in the payload. Thus, when the IP address is added to a packet, the sequence number of each of the subsequent packets needs to be incremented by the count of the added bytes. Further, an acknowledgement sequence number (ack\_seq) in the header on the packets returned from the proxy or the origin server that logically follow receipt of the GET packet(s) at the origin server needs to be decremented by the proxy redirector before being forwarded to the client to avoid confusing the client with respect to what the sequence number of the next byte it sends should be. Further, if the GET request sent by the client encompasses more than one TCP segment, then the extra bytes in the first of the segments caused by the additional bytes added to the URL are shifted into the second segment, and the resultant now extra bytes in the second segment are shifted into the third segment, etc., until the last of the segments. In order to preclude the necessity of requiring an extra segment to be added to the GET request to accommodate the extra bytes, the client sending the GET request, is deceived into sending segments whose maximum size is less than what can actually be received by the proxy as indicated by a maximum segment size (MSS) field in packets from the proxy. The proxy redirector, upon receipt of the On, ACK SYN packet from the proxy, reduces the MSS parameter received from the proxy by the amount of the number of bytes that will be added to the GET request before that parameter is forwarded to the client. Thus, when the client next sends a GET request, each segment is limited to the reduced MSS, thereby insuring that the segment size of a last segment in a GET request after the IP address is prefixed by the proxy redirector to form the absolute URL (whether the GET request is one or more segments long) is less than or equal to the actual MSS that the proxy can receive. (Column 5, line 10 through Column 6, line 4).

In the present invention, that programmable network element is operative in combination with a gateway program that manipulates the destination and source addresses of packets flowing there through in a manner to be described, as well as modifying, as will be described, information in the packet(s) containing the GET request that specifies the URL of the requested object. Specifically, the programmable network element in combination with the gateway program operates on packets associated with HTTP requests, which are determined from the destination port number. As previously noted, HTTP requests are conventionally addressed to port 80 of an origin server. Thus, the programmable network element/gateway program which together comprise proxy redirector 104 in this embodiment, captures through the dispatcher process of the programmable network element, packets directed to port 80 and then performs address translations on those captured packets to readdress these packets to a selected proxy. With respect to address translations, the gateway program translates the destination IP address of packets addressed to the origin server to the IP address of a selected proxy cache and translates the source IP address of such packets from that of the client to the IP address of proxy redirector 104. Further, in order for proxy redirector 104 to identify requests from plural client terminals that are directed to the same proxy, the source port number is translated to a bogus ghost port number at the proxy redirector. Thus, when proxy cache responds, the packets transmitted by the cache have a destination IP address of proxy redirector 104 at that bogus port number, which is distinctly associated with the client. The gateway program within proxy redirector 104 then translates the IP destination address of these responsive packets from the proxy to the IP address of the client and translates the bogus destination port number to the port number from which the client originated its request. Further, the gateway program translates the source IP address of such responsive packets from that of the proxy to the IP address of the origin server and the port number to the port (80) to which the client's requests were originally directed. Thus, the packets which are returned to the client from the proxy masquerade as if they had originated from the origin server to which the client "believed" its request had been sent. (Column 8, lines 11-52).

**V. The Proposed Combinations of *Hokari*, *Civanlar*, and *Cohen* Fail to Disclose, Teach, or Suggest Various Limitations Recited in Appellants' Claims**

Claims 1-35 and 37-46 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the relied upon combinations of *Hokari*, *Civanlar*, and *Cohen*. Appellants respectfully submit, however, that Claims 1-35 and 37-46 are clearly patentable over the proposed *Kisor-Berger* combination. Appellants respectfully submit that these rejections are, therefore, improper and should be reversed by the Board.

**A. Group 1 (Claims 1-3, 6, 8-11, 13-20, 23-27, 30, 31-35, 37, 38,40-43, and 45)**

Claims 1-3, 6, 8-11, 13-20, 23-27, 30, 31-35, 37, 38,40-43, and 45 stand rejected under 35 U.S.C. § 103(a) as being anticipated by the *Hokari-Civanlar-Cohen* combination.

**1. The Claims of Group 1 are Allowable over the Proposed *Hokari-Civanlar-Cohen* Combination**

First, Appellants respectfully submit, however, that the *Hokari-Civanlar-Cohen* combination does not disclose, teach, or suggest each and every element recited in Appellants' Claims 1-3, 6, 8-11, 13-20, 23-27, 30, 31-35, 37, 38,40-43, and 45. For example, independent Claim 1 recites a method for establishing a telephone call between a trusted Internet Protocol (IP) telephone and an untrusted device that includes, *inter alia*:

receiving a call initiation request from an untrusted device external to a trusted network, the call initiation request indicating a desired communication with a trusted IP telephone coupled to the trusted network;

evaluating the call initiation request;

establishing a telecommunication link between the untrusted device and the trusted IP telephone in response to a positive evaluation of the call initiation request, wherein evaluating the call initiation request comprises determining whether the untrusted device is requesting the establishment of media streaming with the trusted IP telephone;

monitoring communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are

media streaming to maintain the integrity of the trusted network;  
and

terminating the telecommunication link if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming to maintain the integrity of the trusted network.

Thus, independent Claim 1 recites the following combination of features and operations: (1) establishing a telecommunication link; (2) monitoring communications transmitted . . . on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network; and (3) terminating the telecommunication link if the communications transmitted . . . are not media streaming to maintain the integrity of the trusted network. Appellants respectfully submit, however, that the *Hokari-Civanlar-Cohen* combination does not disclose, teach, or suggest the recited combination of features and operations.

The M.P.E.P. provides that “[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art.” M.P.E.P. § 2143.03 (citing *In re Wilson*, 424 F.2d 1382, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970)). In the Final Office Action, the Examiner acknowledges that *Hokari* does not disclose media streaming or “monitoring the type of streaming” but maintains that *Hokari* discloses “monitoring data streaming,” generally. (Office Action, pages 2 and 4-5). The Examiner then relies upon *Civanlar* for the disclosure of “media streaming,” specifically. (Office Action, page 5). The Examiner does not identify any reference, however, that explicitly discloses the combination of features recited by Appellants’ step of “**monitoring communications transmitted . . . on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network.**” In fact, in maintaining the rejection of the recited claim language using the identified portions of *Hokari* and *Civanlar*, Appellants respectfully submit that the Examiner has merely pieced together disjointed portions of unrelated references to reconstruct Appellants’ claim. Appellants further submit that such a piecemeal rejection fails to consider the particular combination of features recited in Appellants’ Claim 1 and, thus, fails to give credence to each element of Appellants’ claim. Because the Examiner has not shown where the combination of elements is disclosed in *Hokari*, *Civanlar*, or *Cohen*, Appellants submit that the rejection of Claim 1 is improper and should be withdrawn.

Furthermore, to the extent that *Hokari* discloses “monitoring data streaming” as suggested by the Examiner, such monitoring is not the analogous to Appellants’ steps of “establishing a telecommunication link” and then “monitoring communications transmitted . . . on the telecommunication link . . . to maintain the integrity of the trusted network,” as recited in Claim 1. Rather, *Hokari* is limited to a system for processing a set-up message to connect a call. Specifically, and as summarized above, *Hokari* discloses, that “[w]hen a dial number is received from the public network subscriber 106 (S1021), the PBX 102 decides whether the dial number is a leased line number or not (S1022).” (Column 4, lines 13-16). “If the dial number received is a leased line number (YES of S1022), a set-up message 301 for the public line-leased line connection is formed (S1023-S1025).” (Column 4, lines 16-19). “If it is an ISDN public network number (NO of S1022), a set-up message of the ISDN public network is formed (S1027)” and “is transmitted from the PBX 102 to the ISDN public network 101 (S1025).” Column 4, lines 19-23). Thus, whether the dialed number is a leased line number (identified by a first number of “8” as described in Column 4, lines 24-27) determines the steps to be performed for the formation of an appropriate set-up message, which is then forwarded to the ISDN public network. The formation of a set-up message, however, necessarily occurs prior to the “[establishment] of a telecommunication link between the untrusted device and the trusted IP telephone,” as recited in Applicants’ Claim 1.

For the alleged disclosure of “monitoring data streaming,” the Examiner specifically relies on Column 4, line 51 through Column 5, line 7 of *Hokari*. The cited portions of *Hokari*, however, merely disclose the steps performed by the PBX access point in processing the set-up message 301. As a result, such steps also necessarily occur prior to the establishment of a telecommunication link between the calling party and the called party and, thus, cannot be analogous to Applicants’ step of “monitoring communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network.”

For example, *Hokari* discloses that “the PBX 103 which becomes an access point receives the set-up message 301 having the destination number which is identical to the stored public line-leased line connection number “03-3210-1111” from the ISDN public network 101 (S1030).” (Column 4, lines 51-55). “The access point PBX 103 decides whether the calling party number “03-3210-2222” of the calling subscriber 106 is registered

in the ID table of the main memory 327 (S1031).” (Column 4, lines 55-58). If it is registered, the connection of the call is permitted (S1032) and the leased line number “8-10-2000” is read out from the destination sub-address of the set-up message (S1033).” (Column 4, lines 58-62). “Then, a new set-up message having this leased line number as a destination number is formed and sent to the leased line network 105 to connect the call.” (Column 4, lines 62-64). Thus, *Hokari* explicitly discloses that the described steps are performed before a connection is established. As a result, *Hokari* cannot be said to disclose, teach, or suggest “establishing a telecommunication link,” “monitoring communications transmitted . . . on the telecommunication link . . . to maintain the integrity of the trusted network,” as recited in Claim 1.

As still another example of the deficiencies of the proposed *Hokari-Civanlar-Cohen* combination, Appellants respectfully submit that the cited references do not disclose, teach, or suggest “terminating the telecommunication link if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming to maintain the integrity of the network,” as recited in Claim 1. As demonstrated above, *Hokari* is limited to the processing of a set-up message where the called party is a leased line. Since the steps disclosed in *Hokari* are performed prior to the establishment of a telecommunication link between the called party and the calling party and since the Examiner acknowledges that *Hokari* does not disclose media streaming (Office Action, pages 2 and 4-5), *Hokari* cannot be said to disclose, teach, or suggest Applicants’ step of “terminating the telecommunication link if the communications transmitted between the untrusted device and the trusted device are not media streaming,” as recited in Claim 1.

The additional disclosure of *Civanlar* does not cure the deficiencies of *Hokari* identified above. While *Civanlar* discloses an “IP call set-up interface 101” and “a signaling format translator 104,” neither element operates to “[terminate] the telecommunication link if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming to maintain the integrity of the trusted network,” as recited in Appellants’ Claim 1. Rather, the IP call set-up interface 101 merely “sends and receives call setup requests” and the signaling format translator merely translates “call-setup requests into a form that the interface 101 can properly understand.” (Column 5, lines 55-57; Column 6, lines 8-11). Thus, the “IP call set-up interface 101” and “a signaling format translator 104” are merely involved in the initial setup of the communication session. Even though *Civanlar*

discloses that the “interface 101 monitors the status of each call establishment session and transmits error messages” (Column 6, lines 13-17), there is no indication in *Civanlar* that this “monitoring” extends beyond the initial set up of the communication session.

In the Final Office Action, the Examiner states that *Civanlar* recites [in] column 5, line 50 through column 6 ‘an IP call set-up interface 101 is provided for receiving and terminating call setup requests.’” (Office Action, page 3). Appellants respectfully submit, however, that the termination of a call setup request is not analogous to the termination of an established telecommunication link “if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming,” as recited in Claim 1. Similarly, the Examiner’s reliance upon “IP packet mixer 201” also ignores the context in which the cited portions of *Civanlar* are disclosed. The portion of *Civanlar* relating to “IP packet mixer 201” that is relied upon by the Examiner explicitly discloses that “the IP packet mixer 201 also provides control functionality that would otherwise be performed by the IP call set-up interface 101.” Thus, while IP packet mixer may receive control packets that “identify the control information pertaining to the station from which it receives the packet, such as the type of voice encoding that is employed by the station” (Column 7, lines 22-29), there is no indication that this disclosed functionality of IP packet mixer 201 extends beyond the initial set-up of the call. Furthermore, to the extent that *Civanlar* discloses that “IP packet mixer 201 is also used by an IP station to terminate its participation in a session” (Column 7, lines 31-32), this statement alone or in the context of the preceding disclosure of *Civanlar* cannot be considered to be analogous to Appellants’ step of “terminating the telecommunication link if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming to maintain the integrity of the network,” as recited in Claim 1.

For at least these reasons, Appellants respectfully submit that the proposed *Hokari-Civanlar-Cohen* combination fails to disclose, teach, or suggest each and every limitation recited in Appellants’ independent Claim 1. For at least analogous reasons, Appellants respectfully submit that the rejection of independent Claims 2, 14, 26, and 38 and their respective dependent claims (including Claims 3, 6, 8-11, 13, 15-20, 23-25, 27, 30, 31, 33-35, 37, 40-43, and 45) is improper and should be reversed by the Board.

## **2. The Proposed *Hokari-Civanlar-Cohen* Combination is Improper**

Second, Appellants submit that the Examiner has not demonstrated the requisite teaching, suggestion, or motivation in *Hokari*, *Civanlar*, *Cohen*, or the knowledge generally available to those of ordinary skill in the art at the time of the invention to modify or combine *Hokari*, *Civanlar*, and *Cohen* in the manner the Examiner proposes. The rejections are improper and should be reversed for at least this additional reason.

As discussed above in Section I of this Appeal Brief, the question raised under 35 U.S.C. § 103 is whether the prior art taken as a whole would suggest the claimed invention taken as a whole to one of ordinary skill in the art at the time of the invention. Accordingly, even if all elements of a claim are disclosed in various prior art references, which is certainly not the case here as discussed above, the claimed invention taken as a whole cannot be said to be obvious without some reason given in the prior art why one of ordinary skill at the time of the invention would have been prompted to modify the teachings of a reference or combine the teachings of multiple references to arrive at the claimed invention. It is clear based at least on the many distinctions discussed above that the proposed *Hokari-Civanlar-Cohen* combination does not, taken as a whole, suggest the claimed invention, taken as a whole.

For example, as described above *Hokari* relates to a connection-based telephony system. Specifically, the connection system includes a first PBX for connecting the public network subscriber and the public network, a second PBX for the private network subscriber, and the private network, and third PBXs for connecting the public line and the private line. (Abstract). In contrast, *Cohen* relates a method and apparatus to “transparently redirect an HTTP connection request that is directed to an origin server (107) to a proxy cache (110-1).” (Abstract). The objective of *Cohen* is to “decrease both the latency of object retrieval and traffic on the Internet backbone.” (Column 1, lines 12-14). Thus, in addition to being outside the field of technology of either *Hokari*, the proxy for processing Internet GET requests as described in *Cohen* does not even remotely deal with the same types of problems encountered by connection-based and connectionless telephony systems. Furthermore, there is no explicit or implicit reference in either reference which would suggest to one of ordinary skill to combine the connection-based telephony network of *Hokari* and the method of transparent proxy caching disclosed in *Cohen*.

In this respect, Applicants respectfully submit that the references are non-analogous art and, because not related, an improper combination. It certainly would not have been obvious to



one of ordinary skill in the art at the time of the invention, based solely on the cited references, *to even attempt* to incorporate into the connection-based telephony network of *Hokari* an Internet proxy cache such as the one disclosed in *Cohen*. Even more clearly, it certainly would not have been obvious to one of ordinary skill in the art at the time of the invention, based solely on the cited references, *to actually* incorporate into the connection-based telephony network of *Hokari* an Internet proxy cache such as the one disclosed in *Cohen*, which would be required to establish a *prima facie* case of obviousness under the M.P.E.P. and the governing Federal Circuit case law.

Additionally, “the factual inquiry whether to combine references must be thorough and searching.” *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52, 60 U.S.P.Q.2d 1001, 1008 (Fed. Cir. 2001). Thus, the burden is on the Examiner to identify concrete evidence in the record to support his conclusion that it would have been obvious to modify the teachings of the cited references to achieve the claimed invention. *See, In re Kotzab*, 217 F.3d 1365, 1370, 55 U.S.P.Q.2d 1313, 1316-17 (Fed. Cir. 2000). The Examiner’s conclusory assertion that it would have been obvious to combine the teachings of *Hokari* with the teachings of *Cohen* to purportedly arrive at Appellants’ invention is insufficient to support a *prima facie* case of obviousness under 35 U.S.C. § 103(a) under the M.P.E.P. and the governing Federal Circuit case law. Such conclusions made in hindsight using Appellants’ claims as a blueprint, fails to provide a thorough and searching factual inquiry and does not identify any concrete evidence in the record for combining these references in the manner proposed by the Examiner.<sup>2</sup>

Accordingly, since the cited references fail to provide the required teaching, suggestion, or motivation to combine *Hokari* with *Cohen* in the manner the Examiner proposed, Appellants respectfully submit that the Examiner’s conclusions set forth in the Final Office Action fall well short of the requirements set forth in the M.P.E.P. and the governing Federal Circuit case law for demonstrating a *prima facie* case of obviousness. Thus, Appellants respectfully submit that the Examiner’s proposed combination of *Hokari* with *Cohen* appears to be merely an attempt, with the benefit of hindsight, to reconstruct Appellants’ claims and is unsupported by the teachings of *Hokari* and *Cohen*.

---

<sup>2</sup> During prosecution, Appellants requested that if the Examiner was relying on “common knowledge” or “well known” art to combine or modify *Hokari* and *Cohen*, the Examiner provide a reference pursuant to M.P.E.P. § 2144.03 to support such an argument. Appellants also requested that if the Examiner was relying on personal knowledge to supply the required motivation or suggestion to combine or modify *Hokari* and *Cohen*, the Examiner provide an affidavit supporting such facts pursuant to M.P.E.P. § 2144.03. The Examiner did not do so. Appellants respectfully submit that since such a reference or affidavit was not supplied by the Examiner, and since such motivation or suggestion is lacking in the references, the obviousness rejection made by the Examiner was clearly inappropriate.

For at least these reasons, Appellants respectfully submit that the proposed *Hokari-Civanlar-Cohen* combination fails to disclose, teach, or suggest each and every limitation recited in Appellants' independent Claim 1. For at least analogous reasons, Appellants respectfully submit that the rejection of independent Claims 2, 14, 26, and 38 and their respective dependent claims (including Claims 3, 6, 8-11, 13, 15-20, 23-25, 27, 30, 31, 33-35, 37, 40-43, and 45) is improper and should be reversed by the Board.

**B. Group 2 (Claims 4, 28, and 39)**

Claims 4, 28, and 39 stand rejected under 35 U.S.C. § 103(a) as being anticipated by the *Hokari-Civanlar* combination. Appellants respectfully submit, however, that the *Hokari-Civanlar* combination does not disclose, teach, or suggest each and every element recited in Appellants' Claims 4, 28, and 39.

For example, dependent Claim 4 recites that "evaluating the call initiation request comprises determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device." Claims 28 and 39 recite certain analogous features and operations. In the Final Office Action, the Examiner relies upon *Hokari* for disclosure of the recited features. The cited portions of *Hokari* do not support the Examiner's rejection. Specifically, *Hokari* discloses, as an example, that "the number of the calling party" is ISDN number 03-3210-2222. (Column 4, lines 45-47). *Hokari* then discloses that PBX 103, as the access point, "decides whether the calling party number "03-3210-2222" of the calling subscriber 105 is registered in the ID table of the main memory 327 (S1031)." (Column 4, lines 55-58). "If it is registered (YES of S1031), the connection of the call is permitted." (Column 4, lines 58-59). Thus, PBX determines whether to set up the call based on a successful identification of the calling party. *Hokari* does not disclose, teach, or suggest "evaluating the call initiation request comprises determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device," as recited in Claim 4 and analogously recited in Claims 28 and 39.

In a telephone interview with the Examiner on November 17, 2005, the Examiner indicated that *Civanlar* might also or alternatively be used to reject Claims 4, 28, and 39. As support for such a rejection, the Examiner pointed to Column 9, lines 40-42, which states, "Once the proper telephone number is determined, interface 102 sends a Q.931 message to station 600 in step 521 to establish the call." Appellants respectfully disagree, however, that

this portion of *Civanlar* discloses, suggests, or teaches that “evaluating the call initiation request comprises determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device,” as recited in Claim 4 and analogously recited in Claims 28 and 39. As summarized above in Section III of this Appeal Brief, *Civanlar* discloses an apparatus for “establishing a communication session between first and second terminals in communication over a plurality of networks that employ differing transmission standards.” (Abstract). Accordingly, a gateway “provides conversion of the transmission format, control, call signaling, and audio stream (and potentially video and data streams) between different transmission standards.” (Column 3, lines 41-45). In particular, and as disclosed by the portion of the reference identified by the Examiner during the telephone interview, *Civanlar* discloses:

If . . . voice gateway B serves the 800 number of station 600, the address translator interface 105 sends the 800 number to the IP call set-up interface 101 of gateway B in step 515. In step 517, the IP set-up interface 101 of gateway B sends the 800 number to the signaling format interface 104, which in turn constructs an SS7 message and forwards it to the telephony call set-up interface 102. In step 518, the interface 102 sends the SS7 message to the NCP in the signaling network to translate the 800 number into a telephone number. The NCP provides the requested telephone number to the telephony call set-up interface 102. Once the proper telephone number is determined, interface 102 sends a Z.931 message to station 600 in step 521 to establish the call.

(Column 9, lines 28-42). Thus, *Civanlar* merely discloses address translation that includes translating the 800 number into a telephone number for establishment of the call. *Civanlar* does not disclose, teach, or suggest, however, “evaluating the call initiation request comprises determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device,” as recited in Claim 4 and analogously recited in Claims 28 and 39.

For at least these reasons, Appellants respectfully submit that the proposed *Hokari-Civanlar* combination fails to disclose, teach, or suggest each and every limitation recited in Appellants’ Claims 4, 28, and 39. For at least these reasons, Appellants respectfully submit that the rejection of dependent Claims 4, 28, and 39 is improper and should be reversed by the Board.

**C. Group 3 (Claims 5 and 29)**

Claims 5 and 29 also stand rejected under 35 U.S.C. § 103(a) as being anticipated by the *Hokari-Civanlar* combination. Appellants respectfully submit, however, that the *Hokari-Civanlar* combination does not disclose, teach, or suggest each and every element recited in Appellants' Claims 5 and 29.

For example, dependent Claim 5 recites that "determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device comprises determining whether a network address of the trusted IP telephone is included in a list of approved network addresses." Claim 29 recites certain analogous features and operations. In the Final Office Action, the Examiner again relies upon *Hokari* for disclosure of the recited features. Appellants have shown above with respect to Claim 4, however, that the cited portions of *Hokari* merely disclose determining whether to set up the call based on a successful identification of the calling party. Specifically, *Hokari* discloses that "the number of the calling party" is ISDN number 03-3210-2222. (Column 4, lines 45-47). *Hokari* then discloses that PBX 103, as the access point, "decides whether the calling party number "03-3210-2222" of the calling subscriber 105 is registered in the ID table of the main memory 327 (S1031)." (Column 4, lines 55-58). "If it is registered (YES of S1031), the connection of the call is permitted." (Column 4, lines 58-59). Thus, *Hokari* does not disclose, teach, or suggest "determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device comprises determining whether a network address of the trusted IP telephone is included in a list of approved network addresses," as recited in Claim 5 and analogously recited in Claim 29.

In the telephone interview with the Examiner on November 17, 2005, the Examiner indicated that *Civanlar* also might be used to reject Claims 5 and 29. As support for such a rejection, the Examiner again directed Appellants' attention to Column 9, lines 40-42, which states, "Once the proper telephone number is determined, interface 102 sends a Q.931 message to station 600 in step 521 to establish the call." For reasons similar to those discussed above with respect to Claim 4, however, Appellants respectfully submit that this portion of *Civanlar* does not disclose, suggest, or teach "determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device comprises determining whether a network address of the trusted IP telephone is included in a list of approved network addresses," as recited in Claim 5 and analogously recited in Claim 29.

Rather, *Civanlar* discloses that “interface 102 sends the SS7 message to the NCP in the signaling network to translate the 800 number into a telephone number.” (Column 9, lines 35-38). “The NCP provides the requested telephone number to the telephony call set-up interface 102. Once the proper telephone number is determined, interface 102 sends a Z.931 message to station 600 in step 521 to establish the call.” (Column 9, lines 38-42). Thus, *Civanlar* also does not disclose, teach, or suggest that “evaluating the call initiation request comprises determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device,” as recited in Claim 5 and analogously recited in Claim 29.

For at least these reasons, Appellants respectfully submit that the proposed *Hokari-Civanlar* combination fails to disclose, teach, or suggest each and every limitation recited in Appellants’ Claims 5 and 29. For at least these reasons, Appellants respectfully submit that the rejection of dependent Claims 5 and 29 is improper and should be reversed by the Board.

***D. Group 4 (Claims 12, 36, and 44)***

Claims 12, 36, and 44 stand rejected under 35 U.S.C. § 103(a) as being anticipated by the *Hokari-Civanlar-Cohen* combination.

**1. The Claims of Group 4 are Allowable over the Proposed  
*Hokari-Civanlar-Cohen* Combination**

First, Appellants respectfully submit that the *Hokari-Civanlar-Cohen* combination does not disclose, teach, or suggest each and every element recited in Appellants’ Claims. Appellants respectfully submit, however, that the *Hokari-Civanlar-Cohen* combination does not disclose, teach, or suggest each and every element recited in Appellants’ Claims 12, 36, and 44. For example, Claim 12 recites that “associating a first logical port of the telephony proxy with the untrusted device comprises associating a User Datagram Protocol (UDP) logical port to enable the streaming of IP packets.” Claims 36 and 44 recite certain analogous limitations.

In the Final Office Action, the Examiner relies upon *Civanlar* for disclosure of the recited features and operations. Specifically, the Examiner relies upon Column 4, lines 8-20. (Final Office Action, page 8). Although the cited portion relates to “connectionless packet switched networks (e.g., the Internet),” there is no disclosure of UDP logical ports or of

“associating a first logical port of the telephony proxy with the untrusted device comprises associating a User Datagram Protocol (UDP) logical port to enable the streaming of IP packets,” as recited in Claims 12, 36, and 44. In fact, the only reference to UDP that Appellants have found within *Civanlar* is in the “Background of the Invention” and merely references UDP headers generally. (“The voice packets carry substantial packetization overhead including the headers of PPP, IP, UDP, and RTP, which can be as big as 40 octets.” (Column 1, lines 55-57).) Certainly, this portion of *Civanlar* cannot be said to disclose, teach, or suggest “associating a first logical port of the telephony proxy with the untrusted device comprises associating a User Datagram Protocol (UDP) logical port to enable the streaming of IP packets,” as recited in Claims 12, 36, and 44.

For at least these reasons, Appellants respectfully submit that the proposed *Hokari-Civanlar-Cohen* combination fails to disclose, teach, or suggest each and every limitation recited in Appellants’ Claims 12, 36, and 44. For at least these reasons, Appellants respectfully submit that the rejections of Claims 12, 36, and 44 are improper and should be reversed by the Board.

## **2. The Proposed *Hokari-Civanlar-Cohen* Combination is Improper**

Second, Appellants submit that the Examiner has not demonstrated the requisite teaching, suggestion, or motivation in *Hokari*, *Civanlar*, *Cohen*, or the knowledge generally available to those of ordinary skill in the art at the time of the invention to modify or combine *Hokari*, *Civanlar*, and *Cohen* in the manner the Examiner proposes. In the interests of brevity and to avoid redundancy, Appellants refer the Board to Sections I and V.A.2 of this Appeal Brief for a discussion of the impropriety of the proposed *Hokari-Civanlar-Cohen* combination. Specifically, for reasons analogous to those discussed above with regard to the claims of Group 1, Appellants submit that the rejections of the claims of Group 2 are improper and should be reversed for at least this additional reason.

### ***E. Group 5 (Claim 21)***

Claim 21 stands rejected under 35 U.S.C. § 103(a) as being anticipated by the *Hokari-Civanlar* combination. Appellants respectfully submit, however, that the *Hokari-Civanlar* combination does not disclose, teach, or suggest each and every element recited in Appellants’ Claim 21. For example, Claim 21 recites “a second trusted network, the

untrusted device coupled to the second trusted network” and “an untrusted network coupling the first trusted network to the second trusted network.”

With respect to Claim 21, the Examiner states that “the additional trusted network is a design choice and does not depart from the spirit and scope of the invention of *Hokari*, which is not limited to one network.” (Office Action, page 12). Thus, the Examiner has asserted, without providing any evidentiary support, that the features of Claim 21 would have been an obvious matter of design choice. Applicant hereby submits that a communication network having the features recited by Claim 21 and incorporated from independent Claim 14 (from which Claim 21 depends) is not within the realm of “an obvious design choice,” and also challenges the Examiner’s statement that the features of Claim 21 would have been an obvious matter of design choice. Such a reasoning, without evidentiary support, is analogous to a reliance on common knowledge. However, M.P.E.P. § 2144.03 specifically states that “it is never appropriate to rely solely on ‘common knowledge’ in the art without evidentiary support in the record, as the principal evidence upon which a rejection was based.” [emphasis added] Because Claim 21 is rejected based only on this assertion of common knowledge, which is the principal evidence upon which the rejections are based, the rejection of Claim 21 is clearly improper.

Furthermore, Appellants submit that one of ordinary skill in the art at the time of the invention would not have been motivated to modify *Hokari* in the manner suggested by the Examiner. As discussed above in Section II of this Appeal Brief, *Hokari* relates to a system for connecting a public network subscriber and a private network subscriber, as indicated by the Title, Abstract, and Summary of *Hokari*. In each embodiment disclosed, *Hokari* includes a “first exchange for connecting the public network subscriber and the public network, a second exchange for the private network subscriber and the private network, and a plurality of third exchanges for connecting a public line of the public network and a private line of the private network.” Column 2, lines 14-21). Stated differently, the very objective of *Hokari* is to allow communication between a **public network subscriber** and a **private network subscriber**. There is no indication in *Hokari* at all of a “a second trusted network, the untrusted device coupled to the second trusted network” and “an untrusted network coupling the first trusted network to the second trusted network,” as recited in Appellants’ Claim 21. Thus, Appellants submit that one of ordinary skill in the art would not have been motivated to modify *Hokari* in the manner proposed by the Examiner.

For at least these reasons, Appellants respectfully submit that the proposed *Hokari-Civanlar* combination fails to disclose, teach, or suggest each and every limitation recited in Appellants' Claim 21. For at least these reasons, Appellants respectfully submit that the rejection of Claim 21 is improper and should be reversed by the Board.




**Conclusion**

Appellants have demonstrated that the present invention, as claimed, is clearly distinguishable over the prior art cited by the Examiner. Therefore, Appellants respectfully request the Board to reverse the final rejections and instruct the Examiner to issue a Notice of Allowance with respect to all pending claims.

Appellants believe that no other fees are due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayment to Deposit Account No. 02-0384 of Baker Botts, L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.  
Attorneys for Appellants

  
Jenni R. Moen  
Reg. No. 52,038  
(214) 953-6809

Date: December 1, 2005

**Correspondence Address:**

Customer No.       **05073**

IN THE CLAIMS:

1. **(Previously Presented)** A method for establishing a telephone call between a trusted Internet Protocol (IP) telephone and an untrusted device, the method comprising:

receiving a call initiation request from an untrusted device external to a trusted network, the call initiation request indicating a desired communication with a trusted IP telephone coupled to the trusted network;

evaluating the call initiation request;

establishing a telecommunication link between the untrusted device and the trusted IP telephone in response to a positive evaluation of the call initiation request, wherein evaluating the call initiation request comprises determining whether the untrusted device is requesting the establishment of media streaming with the trusted IP telephone;

monitoring communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network; and

terminating the telecommunication link if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming to maintain the integrity of the trusted network;

wherein establishing the telecommunication link comprises:

associating a first logical port of a telephony proxy with the trusted IP telephone;

associating a second logical port of the telephony proxy with the untrusted device;

receiving first telecommunication data from the untrusted device at the first logical port;

modifying a first source address information in the first telecommunication data to specify the second logical port of the telephony proxy;

communicating the first telecommunication data with the modified first source address information to the trusted IP telephone;

receiving second telecommunication data from the trusted IP telephone at the second logical port;

modifying a second source address information in the second telecommunication data to specify the first logical port of the telephony proxy; and  
communicating the second telecommunication data with the modified second source address information to the untrusted device.

2. **(Previously Presented)** A method for establishing a telephone call between a trusted Internet Protocol (IP) telephone and an untrusted device, the method comprising:

receiving a call initiation request from an untrusted device external to a trusted network, the call initiation request indicating a desired communication with a trusted IP telephone coupled to the trusted network;

evaluating the call initiation request;

establishing a telecommunication link between the untrusted device and the trusted IP telephone in response to a positive evaluation of the call initiation request;

monitoring communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network; and

terminating the telecommunication link if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming to maintain the integrity of the trusted network;

wherein evaluating the call initiation request comprises determining whether the untrusted device is requesting the establishment of media streaming with the trusted IP telephone.

3. **(Previously Presented)** The method of Claim 2, wherein receiving a call initiation request from the untrusted device comprises intercepting a call initiation request at an entry point to the trusted network servicing the trusted IP telephone, the call initiation request sent from outside the trusted network by the untrusted device.

4. **(Original)** The method of Claim 2, wherein evaluating the call initiation request comprises determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device.

5. **(Original)** The method of Claim 4, wherein determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device comprises determining whether a network address of the trusted IP telephone is included in a list of approved network addresses.

6. **(Original)** The method of Claim 2, wherein evaluating the call initiation request comprises determining whether a network address of the untrusted device is included in a list of approved network addresses.

7. **(Canceled)**

8. **(Original)** The method of Claim 2, wherein establishing a telecommunication link between the untrusted device and the trusted IP telephone comprises establishing a telecommunication link using a telephony proxy, whereby all telecommunications between the trusted IP telephone and the untrusted device are communicated through the telephony proxy.

9. **(Original)** The method of Claim 8, further comprising monitoring the telecommunication link to determine whether the telecommunications being sent by the untrusted device use an appropriate audio format.

10. **(Previously Presented)** The method of Claim 8, wherein monitoring the communications transmitted between the untrusted device and the trusted IP telephone comprises monitoring the telecommunication link to determine whether the telecommunications being sent by the untrusted device comprise media streaming.

11. **(Original)** The method of Claim 8, wherein establishing a telecommunication link between the untrusted device and the trusted IP telephone using the telephony proxy comprises:

associating a first logical port of the telephony proxy with the trusted IP telephone;  
receiving telecommunication data from the untrusted device at the first logical port;  
modifying source address information in the received telecommunication data to specify a second logical port of the telephony proxy associated with the untrusted device; and  
communicating the telecommunication data with the modified source address information to the trusted IP telephone.

12. **(Original)** The method of Claim 11, wherein associating a first logical port of the telephony proxy with the untrusted device comprises associating a User Datagram Protocol (UDP) logical port to enable the streaming of IP packets.

13. **(Original)** The method of Claim 12, wherein modifying the source address information in the received telecommunication data comprises modifying a source IP address and a source port in a header of each IP packet.

14. **(Previously Presented)** A communication network for establishing a telephone call between a trusted telephone and an untrusted device, the communication network comprising:

a first trusted network;

a trusted telephone coupled to the first trusted network;

an authentication controller coupled to the first trusted network and operable to evaluate a call initiation request received from an untrusted device external to the first trusted network, the call initiation request indicating a desired communication with the trusted telephone, wherein evaluating the call initiation request comprises determining whether the untrusted device is requesting the establishment of media streaming with the trusted telephone; and

a call manager operable to initiate the creation of a telecommunication link between the trusted telephone and the untrusted device in response to a positive evaluation of the call initiation request;

wherein the authentication controller is further operable to:

monitor communications transmitted between the untrusted device and the trusted telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network; and

terminate the telecommunication link if the communications transmitted between the untrusted device and the trusted telephone are not media streaming to maintain the integrity of the trusted network.

15. **(Original)** The communication network of Claim 14, wherein the call manager is further operable to initiate the creation of a telecommunication link between the trusted telephone and the untrusted device using a telephony proxy, whereby all telecommunications between the trusted telephone and the untrusted device are communicated through the telephony proxy.

16. **(Original)** The communication network of Claim 15, wherein the telephony proxy, the authentication controller, and the call manager comprise software executed on one or more devices in the first trusted network.

17. **(Original)** The communication network of Claim 14, wherein the authentication controller is a component of the call manager.

18. **(Original)** The communication network of Claim 14, wherein:  
the first trusted network comprises an Internet Protocol (IP) network; and  
the trusted telephone comprises an IP telephone.

19. **(Original)** The communication network of Claim 14, wherein the first trusted network and the untrusted device are coupled to the Internet.

20. **(Original)** The communication network of Claim 14, wherein:  
the first trusted network is coupled to the Public Switched Telephone Network (PSTN) using a gateway; and  
the untrusted device is coupled to the PSTN.

21. **(Original)** The communication network of Claim 14, further comprising:  
a second trusted network, the untrusted device coupled to the second trusted network;  
and  
an untrusted network coupling the first trusted network to the second trusted network.

22. **(Original)** The communication network of Claim 14, wherein the authentication controller comprises a list of addresses of network devices permitted to receive telephone calls from untrusted devices, the authentication controller evaluating a call initiation request positively if the call initiation request indicates a desired communication with a network device having an address in the list of network addresses.

23. **(Original)** The communication network of Claim 14, wherein the authentication controller comprises a list of network addresses of untrusted devices permitted to communicate with the trusted telephone, the authentication controller evaluating a call initiation request positively if the call initiation request originates from an untrusted device having an address on the list of network addresses.

24. **(Original)** The communication network of Claim 14, wherein the authentication controller is further operable to monitor the telecommunication link between the trusted telephone and the untrusted device to determine whether telecommunications being sent by the untrusted device use an appropriate audio format.

25. **(Previously Presented)** The communication network of Claim 14, wherein the authentication controller is further operable to monitor the communications transmitted between the untrusted device and the trusted telephone to determine whether telecommunications being sent by the untrusted device comprise media streaming.

26. **(Previously Presented)** Software embodied in a computer-readable medium and operable to perform the following steps:

receiving a call initiation request from an untrusted device external to a trusted network, the call initiation request indicating a desired communication with a trusted Internet Protocol (IP) telephone coupled to the trusted network;

evaluating the call initiation request;

establishing a telecommunication link between the untrusted device and the trusted IP telephone in response to a positive evaluation of the call initiation request;

monitoring communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network; and

terminating the telecommunication link if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming to maintain the integrity of the trusted network;



wherein evaluating the call initiation request comprises determining whether the untrusted device is requesting the establishment of media streaming with the trusted IP telephone.

27. **(Previously Presented)** The software of Claim 26, wherein receiving a call initiation request from the untrusted device comprises intercepting a call initiation request at an entry point to the trusted network servicing the trusted IP telephone, the call initiation request sent from outside the trusted network by the untrusted device.

28. **(Original)** The software of Claim 26, wherein evaluating the call initiation request comprises determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device.

29. **(Original)** The software of Claim 28, wherein determining whether the trusted IP telephone is a proper recipient of a telephone call from an untrusted device comprises determining whether a network address of the trusted IP telephone is included in a list of approved network addresses.

30. **(Original)** The software of Claim 26, wherein evaluating the call initiation request comprises determining whether a network address of the untrusted device is included in a list of approved network addresses.

31. **(Canceled)**

32. **(Original)** The software of Claim 26, wherein establishing a telecommunication link between the untrusted device and the trusted IP telephone comprises establishing a telecommunication link using a telephony proxy, whereby all telecommunications between the trusted IP telephone and the untrusted device are communicated through the telephony proxy.

33. **(Original)** The software of Claim 32, further operable to monitor the telecommunication link to determine whether the telecommunications being sent by the untrusted device use an appropriate audio format.

34. **(Original)** The software of Claim 32, further operable to monitor the telecommunication link to determine whether the telecommunications being sent by the untrusted device comprise media streaming.

35. **(Original)** The software of Claim 32, wherein establishing a telecommunication link between the untrusted device and the trusted IP telephone using the telephony proxy comprises:

- associating a first logical port of the telephony proxy with the trusted IP telephone;
- receiving telecommunication data from the untrusted device at the first logical port;
- modifying source address information in the received telecommunication data to specify a second logical port of the telephony proxy associated with the untrusted device; and
- communicating the telecommunication data with the modified source address information to the trusted IP telephone.

36. **(Original)** The software of Claim 35, wherein associating a first logical port of the telephony proxy with the untrusted device comprises associating a User Datagram Protocol (UDP) logical port to enable the streaming of IP packets.

37. **(Original)** The software of Claim 36, wherein modifying the source address information in the received telecommunication data comprises modifying a source IP address and a source port in a header of each IP packet.

38. **(Previously Presented)** An apparatus for establishing a telephone call between a trusted Internet Protocol (IP) telephone and an untrusted device, the apparatus comprising:

an authentication controller operable to evaluate a call initiation request received from an untrusted device external to a trusted network, the call initiation request indicating a desired communication with a trusted IP telephone coupled to the trusted network, wherein evaluating the call initiation request comprises determining whether the untrusted device is requesting the establishment of media streaming with the trusted IP telephone;

a call manager operable to:

initiate the creation of a telecommunication link between the trusted IP telephone and the untrusted device in response to a positive evaluation of the call initiation request;

monitor communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network; and

terminate the telecommunication link if the communications transmitted between the untrusted device and the trusted IP telephone are not media streaming to maintain the integrity of the trusted network; and

a telephony proxy, the telecommunication link between the trusted IP telephone and the untrusted device created using the telephony proxy such that all telecommunications between the trusted IP telephone and the untrusted device are communicated through the telephony proxy.

39. **(Original)** The apparatus of Claim 38, wherein the authentication controller comprises a list of addresses of network devices permitted to receive telephone calls from untrusted devices, the authentication controller evaluating a call initiation request positively if the call initiation request indicates a desired communication with a network device having an address in the list of network addresses.

40. **(Original)** The apparatus of Claim 38, wherein the authentication controller comprises a list of network addresses of untrusted devices permitted to communicate with the trusted IP telephone, the authentication controller evaluating a call initiation request positively if the call initiation request originates from an untrusted device having an address on the list of network addresses.

41. **(Original)** The apparatus of Claim 38, wherein the authentication controller is further operable to monitor the telecommunication link between the trusted IP telephone and the untrusted device to determine whether telecommunications being sent by the untrusted device use an appropriate audio format.

42. **(Original)** The apparatus of Claim 38, wherein the authentication controller is further operable to monitor the telecommunication link between the trusted IP telephone and the untrusted device to determine whether telecommunications being sent by the untrusted device comprise media streaming.

43. **(Original)** The apparatus of Claim 38, wherein the telephony proxy comprises:

- a first logical port associated with the trusted IP telephone;
- a second logical port associated with the untrusted device;
- an address modification module operable to modify source address information in telecommunication data received at the first logical port from the untrusted device to specify the second logical port of the telephony proxy; and
- a transmission module operable to communicate the telecommunication data with the modified source address information to the trusted IP telephone.

44. **(Original)** The apparatus of Claim 43, wherein the first and second logical ports are User Datagram Protocol (UDP) logical ports.

45. **(Original)** The apparatus of Claim 43, wherein the address modification module is operable to modify a source IP address and port information in a header of an IP packet.

(19)



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11)

**EP 0 841 831 A2**

(12)

## EUROPEAN PATENT APPLICATION

(43) Date of publication:  
13.05.1998 Bulletin 1998/20

(51) Int Cl.<sup>6</sup>: **H04Q 11/04**, H04L 12/66,  
H04L 29/06, H04L 12/64

(21) Application number: **97308011.2**

(22) Date of filing: **10.10.1997**

(84) Designated Contracting States:  
**AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC  
NL PT SE**  
Designated Extension States:  
**AL LT LV RO SI**

- Coffield, Don Richard  
Locust, New Jersey 07760 (US)
- Leighton, William J., III  
Scotch Plains, New Jersey 07076 (US)
- Mansell, James J.  
Fair Haven, New Jersey 07704 (US)
- Saksena, Vikram R.  
Freehold, New Jersey 07728 (US)

(30) Priority: **07.11.1996 US 743784**

(71) Applicant: **AT&T Corp.**  
**New York, NY 10013-2412 (US)**

(72) Inventors:  
• Civanlar, Seyhan  
Red Bank, New Jersey 07701 (US)

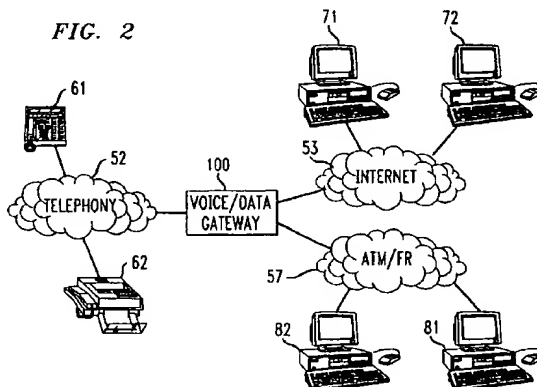
(74) Representative: **Pearce, Anthony Richmond  
MARKS & CLERK,  
Alpha Tower,  
Suffolk Street Queensway  
Birmingham B1 1TT (GB)**

(54) **Wan-based voice gateway**

(57) In one embodiment of the invention, an apparatus is provided for establishing a communication session between first and second terminals in communication over a plurality of networks that employ differing transmission standards. The plurality of networks are selected from among a circuit switched network (e.g., a telephony network), a connectionless packet switched network (e.g., the Internet) and a connection-oriented packet switched network (e.g., an ATM or frame relay network). The apparatus includes a call set-up translator for translating among call set-up protocols associated with the circuit switched network, the connectionless packet switched network and the connection-oriented

packet switched network. An encoding format translator is provided for translating among encoding protocols associated with the circuit switched network, the connectionless packet switched network and the connection-oriented packet switched network. Also provided is an address database for storing a plurality of addresses in different formats for each registered terminal, which includes the first and second terminals. The apparatus also includes a session manager for storing control information relating to the first and second terminals. The control information includes an identification of the first and second terminals that participate in the communication session.

FIG. 2



## Description

### Technical Field

This invention relates generally to an apparatus for establishing communications paths over a circuit switched network, a connectionless packet switched network, and a connection-oriented packet switched network, and more particularly to an apparatus for establishing point-to-point or point-to-multipoint audio or video communication over a telephony network, the Internet, and an Asynchronous Transfer Mode (ATM) or a Frame Relay (FR) network.

### Background of the Invention

Voice traffic transmitted between two or more users over a telephony network is carried over circuit-switched paths that are established between the users. Circuit-switched technology is well-suited for delay-sensitive, real-time applications such as voice transmission since a dedicated path is established. In a circuit-switched network, all the bandwidth of the established path is allocated to the voice traffic for the duration of the call.

In contrast to the telephony network, the Internet is an example of a connectionless packet-switched network that is based on the Internet Protocol (IP). While the majority of the traffic carried over the telephony network is voice traffic, the Internet is more suitable to delay-insensitive applications such as the transmission of data. The Internet community has been exploring improvements in IP so that voice can be carried over IP packets without significant performance degradation. For example, the resource reservation protocol known as RSVP (see RSVP Version 2 Functional Specifications, R. Braden, L. Zhang, D. Estrin, Internet Draft, <draft-ietf-rsvp-spec-06, 1996>) provides a technique for reserving resources (i.e. bandwidth) for the transmission of unicast and multicast data with good scaling and robustness properties. The reserved bandwidth is used to effectively simulate the dedicated bandwidth scheme of circuit-switched networks to transmit delay-sensitive traffic. If RSVP is implemented only for those communications having special Quality of Service (QoS) needs such as minimal delay, the transmission of other communications such as non-real time data packets may be provided to other users of the Internet in the usual best-effort, packet-switched manner.

The majority of Internet users currently access the Internet via slow-speed dial/modem lines using protocols such as SLIP (serial line IP) and PPP (Point to Point Protocol), which run over serial telephone lines (modem and N-ISDN) and carry IP packets. Voice signals are packetized by an audio codec on the user's multimedia PC. The voice packets carry substantial packetization overhead including the headers of PPP, IP, UDP, and RTP, which can be as big as 40 octets. Transmitting voice packets over low speed access lines is almost im-

possible because of the size of the header relative to the size of a typical voice packet (20-160 octets, based on the average acceptable voice delay and amount of voice compression). However, several proposals have emerged to compress the voice packet headers so that greater transmission efficiency and latency can be achieved for voice-packets transmitted over low-speed, dial access lines.

A substantial number of users are expected to begin sending voice traffic over the Internet with acceptable voice quality and latency because of the availability of RSVP and packet-header compression technologies. The transmission terminals for sending packetized voice over the Internet are likely to be multimedia personal computers.

In addition to the telephony network and the Internet, other transmission standards such as Frame-Relay and ATM have been emerging as alternative transport technologies for integrated voice and data. ATM/FR networks are similar to the telephony network in that they both employ connection-oriented technology. However, unlike the telephony network, ATM/FR networks employ packet switching. In contrast to the Internet Protocol, which is a network layer protocol (layer three), FR and ATM pertain to the data link layer (layer two) of the seven-layer OSI model.

Frame Relay and ATM can transport voice in two different formats within the FR (or ATM) packets (cells). In the first format, the FR (ATM) packets (cells) carry an IP packet (or some other layer 3 packet), which in turn encapsulates the voice packets. Alternatively, the FR (ATM) packets (cells) directly encapsulate the voice packet, i.e., without using IP encapsulation. The first alternative employs protocols such as LAN Emulation (LANE), Classical IP Over ATM, and Multiprotocol Over ATM (MPOA), all of which are well known in the prior art. The second alternative is referred to as "Voice over FR" and "Voice over ATM", respectively. Note that the first alternative, which includes IP encapsulation, allows voice packets to be routed between IP routers. That is, layer three processing is performed by the routers along the voice path to determine the next hop router. The second alternative is a purely FR/ATM switched solution. In other words, switching can be performed only at the data link layer. FIG. 1 depicts the protocol stacks for transport of voice over IP and the two alternatives for voice over FR/ATM.

The audio codec depicted in FIG. 1 enables voice encoding/decoding, including voice digitization, compression, silence elimination and formatting. The audio codec is defined by ITU-T standards such as G.711 (PCM of Voice Frequencies), G.722 (7 Khz Audio-Coding within 64 Kbps), G.723 (Dual Rate Speech Code for Multimedia Telecommunications Transmitting at 6.4 and 5.3 Kbps), and G.728 (Speech Encoding at 16 Kbps).

The "Voice over ATM/FR layer" depicted in FIG. 1 is referred to as the multimedia multiplex and synchronization layer, an example of which is defined in ITU-T

standard H.222. ITU-T is currently defining the H.323 standard, which specifies point-to-point and multipoint audio-visual communications between terminals (such as PCs) attached to LANs. This standard defines the components of an H.323 system including H.323 terminals, gate-keepers, and multi-point control units (MCUs). PCs in communication with the Internet can use the H.323 standards to communicate with each other on the same LAN or across routed data networks. In addition to H.323, the ITU-T is in the process of defining similar audio-visual component standards for B-ISDN (ATM) in the H.310 standard, and for N-ISDN in the H.320 standard. The previously mentioned standards also define call signaling formats. For example, IP networks use Q.931 call controls over a new ITU-T standard known as H.225 (for H.323 terminals). Telephony networks use Q.931 signaling and ATM networks use Q.2931 signaling.

Many standards bodies are in the process of defining how voice (and video) can be transported within a given homogenous network such as the telephony, IP, FR and ATM networks. However, there is currently no arrangement for transmitting voice over a heterogeneous network that consists of two or more such networks employing different transmission standards.

### Summary of the Invention

In accordance with the principles of the invention, the foregoing problem can be addressed by employing a WAN-based Voice Gateway which connects to the telephony network, the Internet and the ATM/FR network. Given that network users will be in communication with a variety of such heterogeneous networks, gateway capabilities will be needed between them to support end-point stations in a voice session which are connected to one or more of these different networks. The telephony network, Internet and FR/ATM Networks all use different schemes for establishing a voice session (i.e., call set-up protocols), and different formats for controlling a session and transporting voice. The gateway of the present invention provides conversion of the transmission format, control, call signaling and audio stream (and potentially video and data streams) between different transmission standards. The capabilities of the gateway may also include audio coding translation (e.g., between G.722 and G.728) and address translation between different address types (e.g., a telephone number and an IP address).

In some embodiments of the invention the voice gateway 100 performs the following functions: call-signaling protocol conversion (e.g., between Q.931, Q.2931, H.225); audio mixing/bridging or generation of composite audio and switching; address registration; address translation (e.g., IP <-> E.164 <-> NSAP<-> email); audio format conversion (e.g., from G.711 to G.728); session management/control (e.g. manage number of end points in a call); interfacing with other

gateways (e.g. WAN-to-WAN or WAN-to-local); interfacing with the SS7 signaling network; and interfacing with the Internet signaling network.

In one embodiment of the invention, an apparatus is provided for establishing a communication session between first and second terminals in communication over a plurality of networks that employ differing transmission standards. The communication session may be an audio session, a video session or a multimedia session. The plurality of networks are selected from among a circuit switched network (e.g., a telephony network), a connectionless packet switched network (e.g., the Internet) and a connection-oriented packet switched network (e.g., an ATM or frame relay network). The apparatus includes a call set-up translator for translating among call set-up protocols associated with the circuit switched network, the connectionless packet switched network and the connection-oriented packet switched network. An encoding format translator is provided for translating among encoding protocols associated with the circuit switched network, the connectionless packet switched network and the connection-oriented packet switched network. Also provided is an address database for storing a plurality of addresses in different formats for each registered terminal, which includes the first and second terminals. The apparatus also includes a session manager for storing control information relating to the first and second terminals. The control information includes an identification of the first and second terminals that participate in the communication session.

### Brief Description of the Drawing

In the drawings:

- FIG. 1 shows a simplified protocol stack for transporting voice over an IP network, a telephony network (e.g., an ISDN network) and an ATM/FR network.
- FIG. 2 shows a voice gateway in accordance with the present invention situated among a telephony network, an IP network and a AM/FR network.
- FIG. 3 shows a plurality of voice gateways interfacing with one another and with user terminals.
- FIG. 4 shows a simplified diagram of a voice gateway interconnected with various networks.
- FIG. 5 is a block diagram showing the functionality of various interfaces of which the voice gateway is comprised.
- FIG. 6 shows a flow chart of an exemplary method for processing calls through the voice gateway in accordance with the present invention.
- FIG. 7 is a block diagram of one embodiment of the voice gateway shown in FIGS. 2-4.

### Detailed Description

FIG. 2 shows a voice gateway 100 in accordance with the present invention. As shown, the gateway 100

communicates with networks employing differing transmission standards such as telephony network 52, ATM/FR network 57 and Internet 53. The gateway 100 is connected to a switch, router or server, and an ATM/FR switch, which are located in the telephony network 52, the Internet 53, and the ATM/FR network 57, respectively. The gateway 100 facilitates voice communication between a variety of end-point stations connected to the individual networks. Such stations may include telephone 61, fax machine/telephone 62, and PC 63 (which are connected to the telephony network 52), PCs 71 and 72 (which are connected to the Internet 53) and workstations 81 and 82 (which are connected to the ATM/FR network 57). Voice gateway 100 will be deployed in a distributed fashion. That is, various gateways can be interconnected and used in a tandem manner to complete calls.

The voice gateway 100 includes an interface to each of the networks 52, 53, and 57. These interfaces, depicted in functional form in FIG. 4, will be described below in additional detail. In general, the interfaces serve to convert and manage call signaling among the different networks and to mix voice calls received from within a given network.

As shown in FIG. 3, voice gateway 100 may also be in direct communication with other voice gateways 102 and 103 in the WAN and local voice gateways 105 and 107 attached to the customer's LAN, local ATM/FR networks, or voice terminals. A WAN voice gateway serves as a "master" gateway with respect to local gateways directly attached thereto. In this configuration the local gateways serve as so-called "slaves." When two WAN voice gateways such as gateways 100 and 102 are in direct communication they may act as "peers" with respect to one another while each one also functions as a "master" to the local gateway to which its in direct communication. In an alternative configuration, the WAN voice gateways in direct communication with one another may be arranged in a hierarchical manner in such a way that each WAN voice gateway is connected to another WAN voice gateway that serves as its "master" gateway. A "peer" configuration solution is generally more suitable when the WAN voice gateways are arranged in a mesh-connected topology while the "master" (hierarchical) configuration is generally more suitable for a tree-connected topology. FIG. 3 depicts a mesh-connected topology in which each WAN voice gateway 100, 102, and 103 is a peer of its neighboring WAN gateways.

As seen in FIG. 4, an IP call set-up interface 101 is provided for receiving and terminating call-setup requests from the Internet and for generating call-set up requests to the Internet to establish connections between two or more Internet stations, telephony stations, frame relay stations, and/or ATM stations. Interface 101 sends and receives call setup requests in the form of IP packets using signaling protocols such as Q.931 (or a sub-set of Q.931 as defined in H.323) or another sign-

aling protocol that may be developed particularly for transmitting voice over IP. The IP call set-up interface 101 receives call-setup requests from the telephony call set-up interface 102 (discussed below) in the form of DTMF, Q.931 or other signaling standards. The interface 101 also receives call-setup requests from the ATM/FR call set-up interface 103 (discussed below) if the call-setup request is in the form of Q.2931. A signaling format translator 104 is provided to translate the call-setup requests into a form that the interface 101 can properly understand. The translation is performed before the requests are forwarded to the IP call set-up interface 101. The interface 101 monitors the status of each call establishment session and transmits error messages, as appropriate, in the form of audio messages or digital data to each IP station participating in the session.

The gateway 100 also includes a telephony call set-up interface 102 for receiving call-setup requests from the telephony network 52 or sending call-setup requests to the telephony network 52 to establish connections between two or more Internet stations, telephony stations, frame relay stations and/or ATM stations. Telephony set-up interface 102 receives and sends call setup messages in accordance with Q.931 or with other telephony signaling protocols. The interface 102 also generates SS7 signaling messages to a Network Control Point (NCP) to obtain, for example, a telephone number translation prior to generating an outgoing Q.931 signaling message to the telephony network 52. Additionally, telephony call set-up interface 102 receives call-setup requests from the IP call set-up interface 101 and the ATM/FR call set-up interface 103 (discussed below) if the call-setup request originates in one these networks. The signaling format translator 104 translates the call-set up into a form that is understood by the telephony call set-up interface 102.

Similar to the interfaces 101 and 102 discussed above, an ATM/FR call set-up interface 103 is provided for receiving call-setup requests from the ATM/FR network 57 and for transmitting call-set up requests to the ATM/FR network 57 to establish connections between two or more Internet stations, telephony stations, FR stations, and/or ATM stations. ATM/FR call set-up interface 103 sends and receives call setup requests in the form of packets employing FR/ATM signaling protocols. The ATM/FR call set-up interface 103 also receives call-setup requests from the telephony call set-up interface 102, and the IP call set-up interface 101 if the call-setup request originates in the telephony or IP networks, respectively. The signaling format translator 104 translates these requests into a form of that is understood by the ATM/FR call set-up interface 103.

The gateway 100 further includes an IP packet mixer 201. The IP packet mixer 201 receives voice in the form of IP packet streams from one or more IP stations (including voice terminals or other voice gateways) and processes each incoming stream (e.g., by multiplexing



the various voice streams onto a single IP packet stream). The IP mixer 201 also performs appropriate voice encoding translation into a format compatible with the voice decoding capabilities of each receiving station as identified by the session manager 304. The IP mixer 201 subsequently transmits the IP packets to the other IP stations participating in the session. If there are stations participating in the communication session which are not IP stations, (as identified by the session manager 304), the IP packet mixer 201 sends those packets received from the stations to the format translator 204, which then de-encapsulates and converts the IP packets into a format appropriate for the telephony bridge 202 and/or ATM/FR mixer 203.

In some embodiments of the invention, the IP packet mixer 201 also provides control functionality that would otherwise be performed by the IP call set-up interface 101. In particular, the IP packet mixer 201 performs such control functions when in-band signaling is employed. If out-of-band signaling is employed, the control functions may conveniently reside in the IP call set-up interface 101. In the former situation the IP packet mixer receives control packets over an IP connection such as a dedicated UDP or TCP socket interface, for example. The control packets identify the control information pertaining to the station from which it receives the packet, such as the type of voice encoding that is employed by the station, bandwidth utilization, and QoS requirements. Of course, if no control information is provided, previously defined default control parameters may be used. The IP packet mixer 201 is also used by an IP station to terminate its participation in a session. The session control information received by the IP packet mixer 201 is forwarded to the session manager 304 to maintain a current database of station requirements.

The telephony bridge 202 is the mirror image of the IP packet mixer 201. The bridge 202 bridges (mixes and switches) voice calls received from a plurality of telephony network stations during a voice session. If there are stations participating in the session which are not telephony stations, the bridge 202 sends the digital voice signals it receives from the telephony stations to the voice format interface 204 (discussed below), which performs echo cancellation, voice encoding, encryption and packetization before the digitized voice is sent to the IP mixer 201 and/or the ATM/FR mixer 203 for subsequent forwarding. Telephony bridge 202 also receives calls from voice terminals and other voice gateways.

The ATM/FR mixer 203 is also the mirror image of the IP packet mixer 201. The mixer 203, which bridges voice calls received from a plurality of ATM/FR stations during a voice session, can mix a plurality of different voice streams onto ATM/FR cells/packets. If there are stations participating in the session which are not ATM/FR stations, the mixer sends the ATM/FR voice packets it receives from the ATM/FR stations to the voice format interface 204, which performs any appropriate de-encapsulation, protocol conversion, packetization, etc.,

before the digitized voice is sent to the IP packet mixer 201 and/or the telephony bridge 202 for subsequent forwarding.

The signaling format translator 104 is employed by the gateway 100 to convert and adapt among telephony signaling (Q.931), SS7 signaling, IP call signaling, and FR/ATM signaling protocols. For example, the interface 104 receives signaling messages from the call set-up interface 101 and parses the message, performs appropriate address translation using the address translator 105, and translates the signaling format to another signaling format before sending it to the appropriate outgoing call signaling interface.

The voice format interface is provided to convert and adapt among the various telephony, IP, FR and ATM voice formats, including voice encoding changes, echo cancellation, re-synchronization and packetization.

An address translator 105 is also which allows various stations to register using email address, IP address, E.164 address, MAC address and/or ATM NSAP address formats. The interface can also translate addresses from one address format to another. When multiple gateways are employed, each "master" gateway may collect the address registrations stored in its "slave" gateways. The interface also maintains a list defining the correspondence between the station addresses directly connected to the voice gateway 100.

A session manager interface 304 is employed to receive control information from the mixers, bridges and call set-up interfaces which pertains to the capabilities and status of those stations participating in the communication session. The interface 304 assists the IP mixer 201, telephony bridge 202 and FR/ATM mixer 203 in forwarding voice traffic to all participating stations.

As illustrated in FIG. 5 the voice gateway 100 also connects to various common Operations Administration Management and Provisioning (OAM&P) functions, databases/directories (e.g., authentication databases such as for credit card authorization), and signaling network intelligence that reside within the SS7 signaling network such as a network control point (NCP) and an Internet NCP residing within the Internet. For example, an NCP may be used by the telephony call set-up interface 102 to translate an 800 number into a telephone number. Similarly, an Internet NCP may be used by the IP call set-up interface 101 to request a translation of a station's email address, host name, or URL to an IP. The Internet NCPs provide intelligent services, such as discussed in U.S. Application Serial No. 08/618,483.

FIG. 6 shows a flow chart of an exemplary method for establishing a voice session between the user stations 300 and 600 of FIG. 3 in accordance with the principles of this invention. As seen in FIG. 3, station 300 is provided with direct connectivity to the Internet via voice gateway B. Station 600 communicates with the voice gateway C via an N-ISDN interface. In FIG. 3, the voice gateways A, B and C are all "peers" and any local gateways attached thereto serve as "slaves."

The method begins at step 501 when station 300 sends a call signaling request over the Internet to voice gateway B in the form of an IP packet. The IP packet carries signaling information (e.g., in the form of a Q.931 message), including the IP address of the called station 600. In step 503, the IP call set-up interface 101 parses the IP packet and retrieves the IP address of station 600. In step 505, the IP call set-up interface 101 sends an address query to the address translator 105 to retrieve other addresses for station 600. In step 511, the address translator 105 maps the IP address of station 600 to a toll-free 800 number. Thereafter, at the conditional branch point 513, address translator 105 determines if the 800 number of station 600 is served by voice gateway B.

If the result in step 513 is no, indicating that voice gateway C serves station 600, the method continues with step 523 in which the address translator 105 returns to gateway B to retrieve the IP address of Voice Gateway C for contacting station 600. This step implies that the call to station 600 should be forwarded to voice gateway C, which is the "master" gateway responsible for serving station 600. Thereafter, in step 503, the IP call set-up 101 interface of Voice Gateway B routes the call to the IP call set-up interface 101 of Voice Gateway C for further processing. The method then continues as described below.

If the result in step 513 is YES, indicating that voice gateway B serves the 800 number of station 600, the address translator interface 105 sends the 800 number to the IP call set-up interface 101 of gateway B in step 515. In step 517, the IP set-up interface 101 of gateway B sends the 800 number to the signaling format interface 104, which in turn constructs an SS7 message and forwards it to the telephony call set-up interface 102. In step 519, the interface 102 sends the SS7 message to the NCP in the signaling network to translate the 800 number into a telephone number. The NCP provides the requested telephone number to the telephony call set-up interface 102. Once the proper telephone number is determined, interface 102 sends a Q.931 message to station 600 in step 521 to establish the call.

Once the station 600 is connected, across the Telephony Bridge 202 and IP Mixer 201, a control plane connection is first established between the Users 300 and 600 in step 601 (note that this connection traverses both Voice Gateway C and Voice Gateway B). This connection is employed by both stations in step 603 to indicate their respective audio encoding preferences, say G.711 for station 300 and G.723 for station 600. Note that voice gateway B needs to know the encoding preferences of station 300 while voice gateway C needs to know the encoding preferences of station 600. Additionally, note that the format translation between station 300 and station 600 on the connection plane occurs in voice gateway C (given that communication from voice gateway C to voice gateway B uses IP as the network layer protocol). Once the station capabilities and preferences

are known to each voice gateway in step 605, the session managers 304 in both gateways B and C store a conference table that includes the preferences of both users. Communication proceeds between stations 300 and 600 in step 611 when station 300 sends a voice packet to the IP mixer 201 in gateway B, which in turn sends the packet to the IP mixer 201 in voice gateway C.

The method described above in connection with FIG. 6 may be implemented in a similar manner if station 600 is an ISDN terminal that employs voice over ISDN without implementing the Internet protocol.

FIG. 7 is a block diagram of an exemplary embodiment of WAN-based voice gateway 1001 which includes a) central processing unit (CPU) 1002, b) interface port 1003 c) data bus 1004 and d) memory 1005. Central processing unit (CPU) 1002 provides the computational capability necessary to control the processes of voice gateway 1001. Data bus 1004 provides for the exchange of data between the components of voice gateway 1001. Interface port 1003 provides for the exchange of data between voice gateway 1001 and devices external to Voice Gateway 1001 via link high speed backbone 425. To this end, interface port 1003 contains, for example, well-known data transceivers. Memory 1005 includes 1) code portion 1006, which contains the instructions (program) used by CPU 1002 to control the processes of Voice Gateway 1001, such as those described herein above, and data storage portion 1007, which contains the information necessary to the voice gateway to perform its specific function, such as, address registration and translation.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within its spirit and scope.

#### Claims

1. An apparatus for establishing a communication session between first and second terminals in communication over a plurality of networks employing differing transmission standards, said plurality of networks being selected from among a circuit switched network, a connectionless packet switched network and a connection-oriented packet switched network, comprising:

a call set-up translator for translating among call set-up protocols associated with said circuit switched network, said connectionless packet switched network and said connection-oriented packet switched network;  
an encoding format translator for translating among encoding protocols associated with said circuit switched network, said connectionless

- packet switched network and said connection-oriented packet switched network;  
 an address database for storing a plurality of addresses in different formats for each registered terminal including at least said first and second terminals;  
 a session manager for storing control information relating to the first and second terminals, said control information including an identification of the first and second terminals participating in the communication session.
2. The apparatus of claim 1 wherein said circuit-switched network is a telephony network. 15
  3. The apparatus of claim 1 wherein said connectionless packet switched network is the Internet.
  4. The apparatus of claim 1 wherein said connection-oriented packet switched network is an ATM network. 20
  5. The apparatus of claim 1 wherein said connection-oriented packet switched network is a Frame-Relay network. 25
  6. The apparatus of claim 1 wherein said communication session is established among at least three terminals and further comprising an aggregator for bridging a plurality of communications received from a plurality of the terminals and for transmitting said plurality of communications to remaining ones of said at least three terminals. 30
  7. The apparatus of claim 1 wherein said communication session is an audio session. 35
  8. The apparatus of claim 1 wherein said communication session includes video information. 40
  9. The apparatus of claim 1 wherein said communication session is a multimedia session including audio and video information.
  10. The apparatus of claim 1 wherein said encoding format translator is an audio format translator. 45
  11. The apparatus of claim 1 wherein said encoding format translator is a video format translator. 50
  12. The apparatus of claim 1 wherein said encoding format translator is a multimedia format translator.
  13. The apparatus of claim 1 wherein said control information further includes quality of service requirements. 55
  14. The apparatus of claim 1 wherein said control information further includes information defining a format in which data is to be received by at least one of the first and second terminals.
  15. The apparatus of claim 14 wherein said data format is alterable during the communication session.
  16. The apparatus of claim 1 wherein said call set-up translator translates among a plurality of standards, including H.225, Q.931, Q.2931, and SS7 signaling standards.
- a call set-up translator for translating among call set-up protocols associated with said circuit switched network, said connectionless packet switched network and said connection-oriented packet switched network;  
 an encoding format translator for translating among encoding protocols associated with said circuit switched network, said connectionless packet switched network and said connection-oriented packet switched network;  
 an address database for storing a plurality of addresses in different formats for each registered terminal including at least said first and second terminals;  
 a session manager for storing control information relating to the first and second terminals, said control information including an identification of the first and second terminals participating in the communication session.

FIG. 1

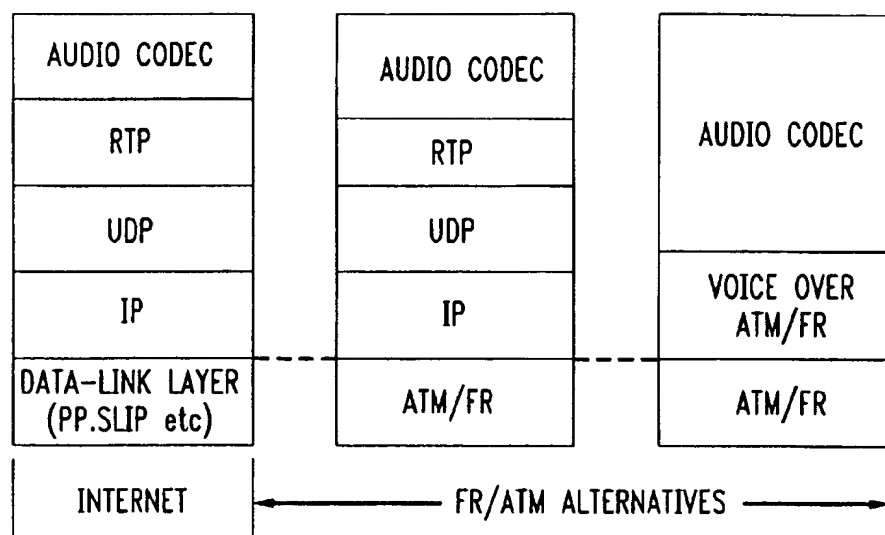


FIG. 2

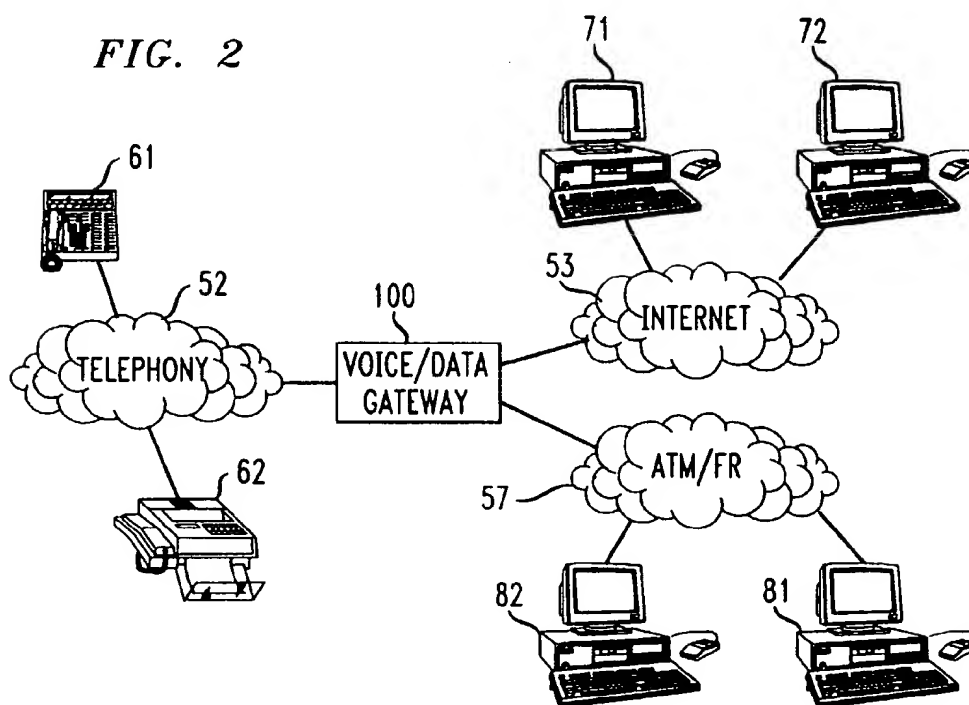


FIG. 3

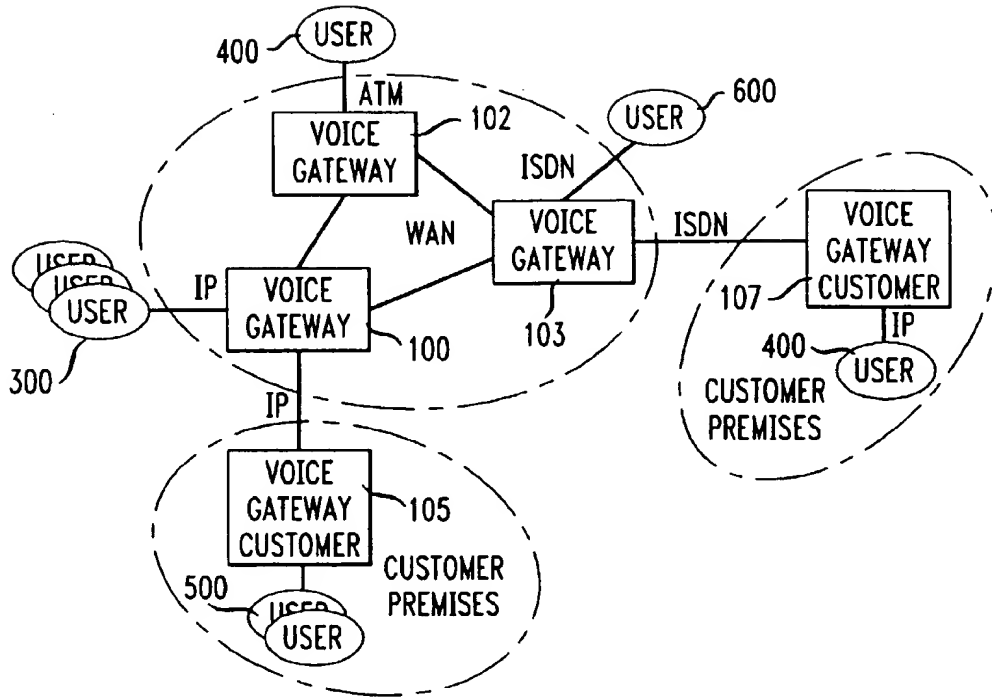
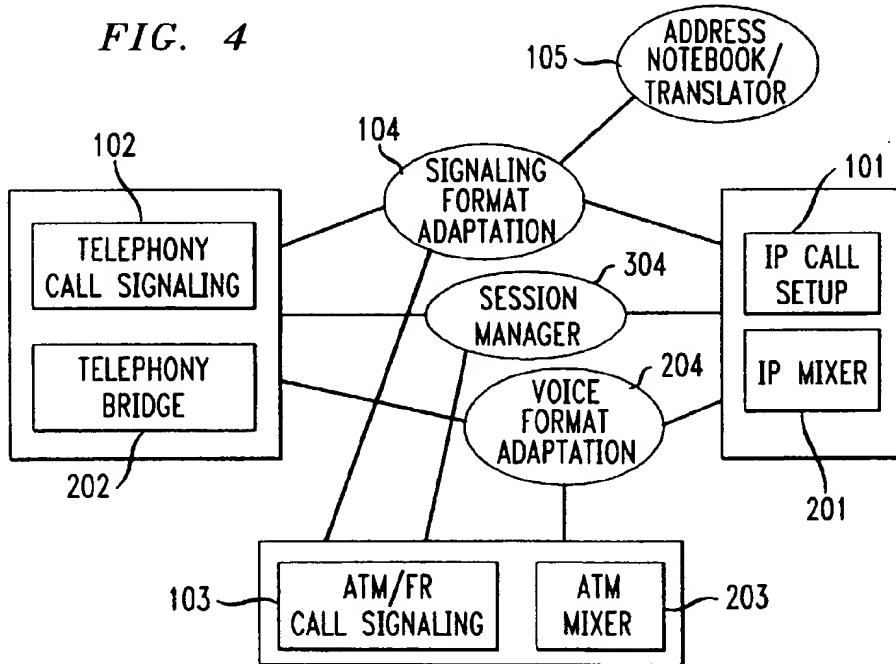


FIG. 4



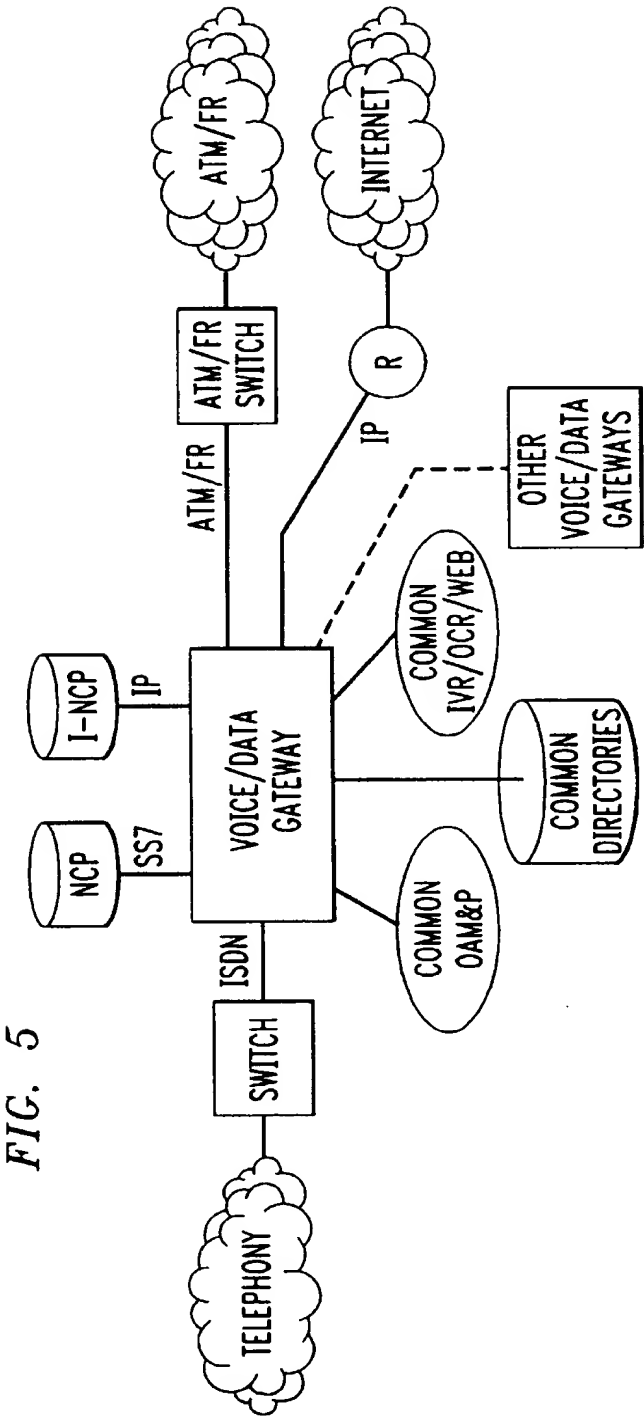
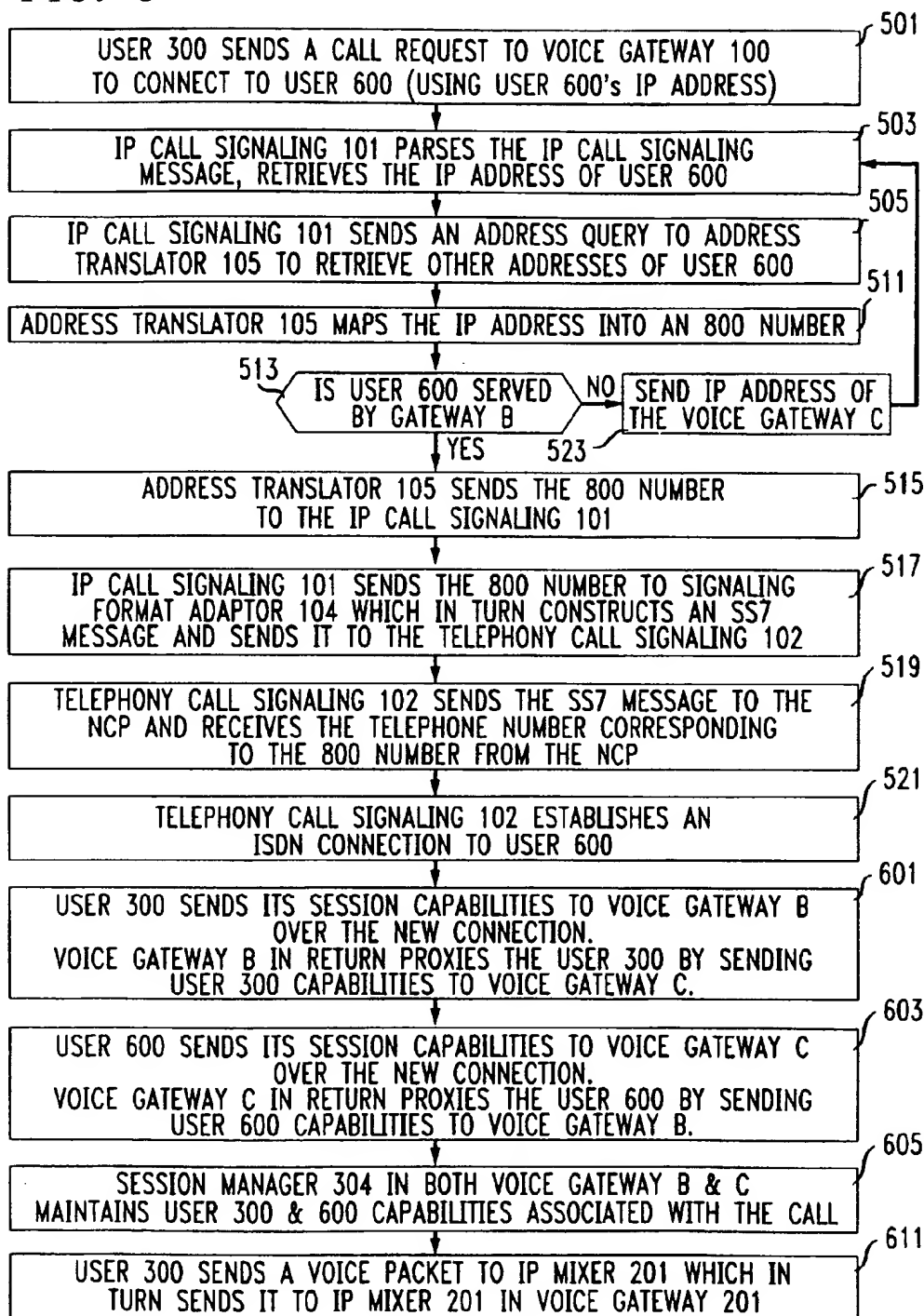
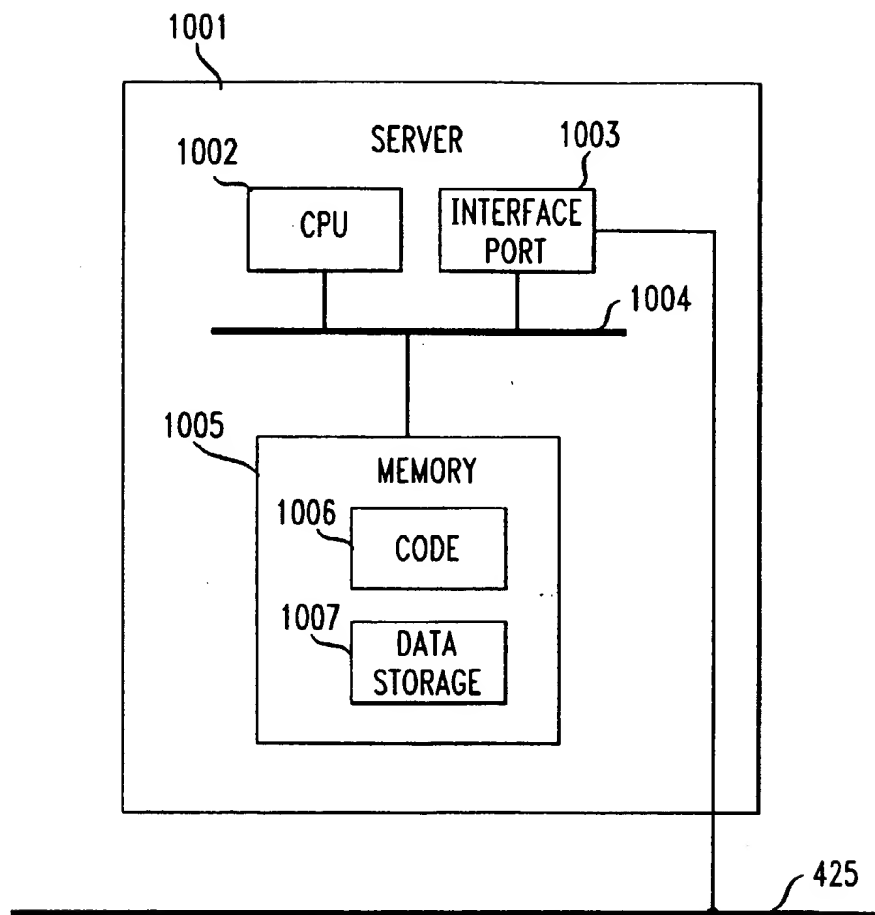


FIG. 6



*FIG. 7*





**Appendix D**

***Evidence Appendix***

Other than the references attached to this Appeal Brief as Appendices B-C, no evidence was submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, and no other evidence was entered by the Examiner and relied upon by Appellants in the Appeal.

**Appendix E**

***Related Proceedings Appendix***

As stated on page 3 of this Appeal Brief, to the knowledge of Appellants' Counsel, there are no known appeals, interferences, or judicial proceedings that will directly affect or be directly affected by or have a bearing on the Board's decision regarding this Appeal.



ATTORNEYS DOCKET  
62891.0292

PATENT APPLICATION  
09/477,193

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: James R. Tighe, et al.  
Serial No.: 09/477,193  
Filing Date: January 4, 2000  
Group Art Unit: 2136  
Examiner: Carl G. Colin  
Title: SYSTEM AND METHOD FOR PROVIDING SECURITY IN  
A TELECOMMUNICATION NETWORK

Mail Stop Appeal Brief Patent  
Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

**CERTIFICATE OF MAILING BY EXPRESS MAIL**

I hereby certify that the attached Appeal Brief (80 pages), check in the amount of \$500.00, Baker Botts return postcard (1 postcard), and this Certificate of Mailing are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on this 1st of December 2005 and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

*Willie Jiles*  
\_\_\_\_\_  
Willie Jiles

Express Mail Receipt  
No. EV 732499374 US